Bibliothèque et Archives Canada | Library and Archives Canada

Canada

LIGNES DIRECTRICES
POUR LA GESTION DES COURRIELS

BIBLIOTHÈQUE ET ARCHIVES CANADA

Direction des documents gouvernementaux

2008

Table des matières

0. Introduction aux lignes directrices pour la gestion des courriels 1

0.1. Références 1
0.2. Lignes directrices 3
0.3. Pourquoi ces lignes directrices s'appliquent-elles à tout le monde? 3
0.4. Quels sont les résultats attendus? 4
0.5. Pourquoi la gestion des courriels est-elle si importante? 5
0.6. Domaines où les lignes directrices ne s'appliquent pas 5
0.7. Feuille de route pour se conformer aux lignes directrices 6
0.8. Cycle de vie de l'information électronique 6
0.9. Définitions 7

1. Les institutions doivent se doter d'un plan pour gérer les courriels 16

1.1. Gérer les programmes et les systèmes de courriel de manière intégrée 17
1.2. Offrir des programmes de sensibilisation et de formation à la gestion des courriels 17
1.3. Utiliser divers supports pour sensibiliser et former à la gestion des courriels 18
1.4. Vérifier que les Lignes directrices pour la gestion des courriels, ainsi que les politiques et procédures associées, ont été bien distribuées, lues et comprises 18
1.5. Conserver des dossiers sur les activités de formation et sur la participation 18

2. Les institutions doivent recueillir et conserver tous les courriels relatifs à leurs activités organisationnelles 20

2.1. Créer, expédier et stocker les courriels de manière structurée 21
2.2. Recevoir et stocker les courriels de manière structurée 22
2.3. Gérer les boîtes aux lettres et les dossiers individuels sur une base régulière 23
2.4. Garder un seul exemplaire de chaque courriel 24
2.5. Gérer et conserver les pièces jointes aux courriels 24
2.6. Considérer les courriels comme des biens, soumis au contrôle juridique du gouvernement du Canada 25
2.7. Utiliser avec modération les listes de diffusion institutionnelles 26
2.8. Fournir un bloc-signature et les coordonnées de la personne-ressource 26
2.9. Ajouter un avis de confidentialité ou de non-responsabilité, s'il y a lieu 27
2.10. Ajouter un avis d'opinion personnelle, s'il y a lieu 27
2.11. Éviter d'utiliser la fonction « Répondre à tous » 28

3. Les institutions doivent classer les courriels relatifs à leurs activités selon un plan de classification basé sur leurs exigences organisationnelles 29

3.1. Maintenir et utiliser un système structuré et efficace de classement des courriels 29
3.2. Déterminer où classer la copie « officielle » 30
3.3. Conserver les métadonnées associées aux courriels 30
3.4. Classifier et classer les courriels systématiquement et fréquemment 31
3.5. Gérer le stockage en ligne temporaire des courriels 31
3.6. Utiliser à une seule fin les boîtes aux lettres communes ou publiques et les dossiers de courriels 32
3.7. Limiter le contenu des courriels à un seul sujet 32
3.8. Décrire l'objet d'un courriel en termes clairs et significatifs 33
3.9. Prévoir un système d'indexation des courriels 33
3.10. Prévoir un mécanisme permettant de suivre le fil conducteur reliant les courriels entre eux (*threading*) 33

4. Les institutions doivent veiller à ce que l'utilisation du courriel contribue à la réalisation d'activités correspondant à leurs objectifs organisationnels 34

4.1. Ne pas utiliser le courriel pour traiter de sujets sensibles, personnels, protégés ou secrets, sauf dans les cas autorisés et en respectant les normes de sécurité en vigueur 35
4.2. Utiliser les journaux d'exploitation pour créer une piste de vérification et veiller au respect des règles 35
4.3. Afficher les noms dans les en-têtes et les adresses de courriel 35
4.4. Être prêt à divulguer un courriel en preuve, sous forme électronique 36
4.5. Surveiller la performance des activités de découverte et de disposition des courriels 36

5. Les institutions doivent veiller à ce que leurs courriels soient maintenus, protégés et conservés selon des calendriers de conservation appropriés 38

5.1. Éviter de procéder à des purges indiscriminées dans les systèmes de courriel 39
5.2. Gérer les courriels de façon à en permettre l'accès aux personnes autorisées 39
5.3. Enlever le chiffrement avant de quitter une institution 40
5.4. Enlever le chiffrement avant de transférer les courriels à Bibliothèque et Archives Canada 40
5.5. Garantir la sécurité des systèmes qui soutiennent les fonctions de courriel 40
5.6. Utiliser des mots de passe, les changer régulièrement et les garder secrets 41
5.7. Protéger les systèmes contre les pertes ou les dommages 42
5.8. Employer le bon niveau de classification de sécurité 43
5.9. Établir des processus obligatoires pour créer, supprimer et suspendre les comptes de courriel au moment opportun 43
5.10. Contrôler les droits d'accès aux comptes et aux dossiers de courriel 44
5.11. Utiliser des mesures de protection et d'authentification des messages 45

5.12. Effectuer régulièrement des copies de sécurité aux fins de récupération en cas de sinistre 45
5.13. Utiliser la signature numérique s'il y a lieu 46
5.14. Enlever les signatures numériques servant à empêcher l'accès aux courriels avant de les transférer à Bibliothèque et Archives Canada 46
5.15. Ne pas employer de signature numérisée pour signer un courriel 46
5.16. Utiliser le chiffrement s'il y a lieu 47
5.17. Employer le stockage de proximité pour la conservation à long terme des courriels 47
5.18. Éviter de conserver des copies papier de courriels dont l'original électronique existe encore 48
5.19. Protéger les courriels en protégeant les supports de conservation 48
5.20. Protéger les courriels de l'obsolescence 48
5.21. Constituer, tenir à jour et conserver une documentation relative au système de courriel 49
5.22. Conserver en permanence la documentation du système de courriel 49
5.23. Gérer des délais de conservation différents pour les courriels et leurs pièces jointes 49
5.24. Appliquer un ordre de retenue, au besoin, pour retarder l'élimination d'un document 50

6. Les institutions doivent disposer de leurs courriels conformément aux lois et politiques pertinentes 51

6.1. Obtenir une autorisation de disposition des courriels 51
6.2. Éliminer les copies de courriels (incluant les copies latentes) au moment opportun 52
6.3. Empêcher la destruction ou la modification de documents qui pourraient être requis dans le cadre d'un audit, d'une action en justice ou de l'AIPRP 52

7. Les institutions doivent réexaminer périodiquement l'efficacité de leurs politiques et pratiques en matière de courriel et apporter des améliorations au besoin 53

7.1. Évaluer l'efficacité de la gestion des courriels 53

8. Chaque personne oeuvrant au sein du gouvernement fédéral doit comprendre ses responsabilités en matière de gestion des courriels 54

8.1. Responsabilités des utilisateurs 54
8.2. Responsabilités des administrateurs de réseaux ou de systèmes 55
8.3. Responsabilités des spécialistes en gestion de l'information 55
8.4. Responsabilités des gestionnaires des opérations 56
8.5. Responsabilités des dirigeants 57

Annexes

ANNEXE A. RÔLES ET RESPONSABILITÉS

0. Introduction aux lignes directrices pour la gestion des courriels

0.1. Références

0.1.1 Nom : Lignes directrices pour la gestion des courriels

0.1.2 Catégorie : Lignes directrices

0.1.3 Autorisation : Bibliothèque et Archives Canada

0.1.4 Organisme responsable : Bibliothèque et Archives Canada

0.1.5 Index croisé

(Documents reliés au sujet : lois, politiques, directives et normes – Gouvernement du Canada, autres sources)

Correspondance entre les lois et politiques et le Cadre de la gestion de l'information Lois et politiques reliées au cycle de vie de l'information				
Lois et politiques	Création Saisie	Organisation Utilisation Diffusion	Tenue à jour et préservation	Disposition
Accès à l'information, Loi et règlements sur l'	X	X	X	X
Accès à l'information, Politique sur l'	X	X	X	X
Apprentissage, de formation et de perfectionnement, Politique en matière d'				
Autorisation et l'authentification électroniques, Politique sur l'			X	
Bibliothèque et les Archives du Canada, Loi sur la	X	X	X	X
Charte canadienne des droits et libertés		X		
Communication, Politique de	X	X	X	X
Droit d'auteur, Loi sur le			X	
Emploi dans la fonction publique, Loi sur l'		X		
Évaluation, Politique d'			X	
Évaluation des facteurs relatifs à la vie privée, Politique d'	X	X	X	X
Gestion de l'information, Politique sur la	X	X	X	X

Correspondance entre les lois et politiques et le Cadre de la gestion de l'information Lois et politiques reliées au cycle de vie de l'information				
Lois et politiques	Création Saisie	Organisation Utilisation Diffusion	Tenue à jour et préservation	Disposition
Gestion de l'infrastructure à clé publique, Politique de			X	
Gestion des finances publiques, Loi sur la	X	X	X	
Gestion des projets, Politique sur la		X		
Gestion des risques, Politique sur la			X	
Gestion des technologies de l'information, Politique sur la	X		X	
Langues officielles, Loi sur les		X		
Preuve au Canada, Loi sur la	X	X	X	
Protection civile, Loi sur la			X	
Protection de l'information, Loi sur la			X	
Protection des renseignements personnels, Loi et règlements sur la	X	X	X	X
Protection des renseignements personnels, Politique sur la	X	X	X	
Protection des renseignements personnels et des documents électroniques, Loi sur la	X	X	X	X
Responsabilité civile de l'État et le contentieux administratif, Loi sur la			X	
Rôles et responsabilités en matière de gestion de l'information, Directive sur les	X	X	X	X
Sécurité, Politique sur la		X	X	
Service canadien du renseignement de sécurité, Loi sur le	X	X	X	
Services communs, Politique sur les	X	X		
Statistique, Loi sur la	X	X	X	
Utilisation des réseaux électroniques, Politique d'		X	X	
Vérificateur général, Loi sur le		X		

(Source : http://www.tbs-sct.gc.ca/fmi-cgi/foundation-fondement/leg-reg/leg-reg09_f.asp)

0.2. Lignes directrices

Vous êtes sur le point d'entreprendre la lecture d'un document contenant des lignes directrices relatives à la gestion des courriels dans l'ensemble du gouvernement canadien. Chacune de ces lignes directrices comporte une ou plusieurs recommandations afin de vous aider à obtenir les résultats attendus.

Ces lignes directrices et les recommandations associées ne sont pas obligatoires, mais elles se veulent une référence, un modèle d'excellence.

0.3. Pourquoi ces lignes directrices s'appliquent-elles à tout le monde?

En vertu de la Politique de gestion de l'information, les ministères et organismes (ci-après « les institutions ») du gouvernement fédéral doivent recueillir, créer, recevoir et saisir tous les documents relatifs à leurs activités organisationnelles, incluant les messages électroniques (courriels) qui contiennent de l'information faisant partie de la mémoire institutionnelle ou des données utilisées pour prendre une décision ou entreprendre une action. La Politique de gestion de l'information et la Directive sur les rôles et responsabilités en matière de gestion de l'information identifient des responsabilités précises pour tous les employés du gouvernement.

L'administrateur général est responsable devant son ministre et le Conseil du Trésor d'une gestion efficace et bien coordonnée de l'information pour l'ensemble de son ministère. Chaque employé du gouvernement, sans exception, a un rôle à jouer dans la gestion des courriels.

Pour donner de bons résultats, les Lignes directrices pour la gestion des courriels doivent s'intéresser aux interventions humaines autant qu'aux systèmes électroniques. En d'autres mots, les machines sont incapables de prendre toutes les décisions que suppose la gestion des courriels.

Les dirigeants trouveront, dans les présentes lignes directrices, des ressources pour les aider à intégrer les exigences de la gestion de l'information dans toutes les activités de conception, de mise en œuvre, d'évaluation et de rapport découlant des programmes et services de leur organisation.

Les spécialistes en technologies de l'information peuvent s'attendre à trouver dans ces lignes directrices des normes et des orientations relatives à la configuration et au fonctionnement des ordinateurs et des réseaux (équipements et logiciels) qui sous-tendent les courriels.

Les spécialistes en gestion de l'information trouveront ici des orientations concernant la gestion des courriels à toutes les étapes de leur cycle de vie : création ou réception, classement, stockage, récupération et disposition.

Le personnel professionnel, les contractuels et les autres utilisateurs de courriel trouveront dans ces lignes directrices et les recommandations associées des éléments d'orientation non techniques dont ils devront tenir compte chaque fois qu'ils utiliseront leur courriel.

Par conséquent, ces lignes directrices s'adressent à un très large public.

- Dirigeants
- Gestionnaires
- Professionnels en gestion de l'information (GI)
- Professionnels en technologie de l'information (TI)
- Utilisateurs du courriel

Ces personnes ont différents rôles à jouer, n'ayant pas toutes le même niveau de connaissance des activités organisationnelles, de compétence technique ou d'autorité. Certaines ont plus d'un rôle à jouer. Ainsi, le dirigeant et le professionnel en TI portent chacun deux chapeaux : l'un est un spécialiste des opérations, l'autre un expert en technologie, mais ce qu'ils ont en commun, et avec tous les autres employés de l'organisation, c'est qu'ils sont aussi des utilisateurs du courriel.

0.4. Quels sont les résultats attendus?

On reconnaît généralement qu'il est impossible de gérer les courriels selon un mode entièrement centralisé. Essentiellement, le processus de gestion du courriel commence avec les utilisateurs, qui doivent chaque jour, à leur écran d'ordinateur, décider quels messages éliminer et quels messages conserver, et où classer ces derniers.

Les lignes directrices et recommandations contenues dans le présent document proposent des procédures visant à garantir la conservation de la bonne information, au bon moment, et pour la bonne période de temps. Notez bien que ce document ne recommande par de délai de conservation particulier pour les courriels. En effet, les délais de conservation varient selon le sujet ou la fonction du courriel et sont établis par chaque institution, conformément aux exigences légales et organisationnelles applicables à cette dernière.

Afin que les utilisateurs soient bien informés quant à la manière de gérer les courriels reçus et envoyés, les dirigeants et les gestionnaires auront droit à des recommandations supplémentaires très précises concernant la formation du personnel et son adhésion à ces lignes directrices.

Les procédures techniques décrites dans le présent document s'adressent aux spécialistes en technologie de l'information (TI) et en gestion de l'information (GI) qui participeront à la mise en place de l'infrastructure technologique appropriée.

Certaines des recommandations formulées dans ces lignes directrices s'adresseront spécifiquement à l'un ou l'autre des groupes mentionnés ci-dessus. D'autres recommandations

s’appliqueront à plus d’un groupe. Dans ce cas, les groupes auront probablement des rôles différents à jouer dans la mise en œuvre des lignes directrices; leurs rôles respectifs seront alors précisés.

0.5. Pourquoi la gestion des courriels est-elle si importante?

Tout simplement parce que le courriel est largement utilisé pour prendre des décisions, assigner des tâches, transmettre des rapports d’étape, confirmer des transactions, et à plusieurs autres fins reliées aux opérations du gouvernement. Les courriels relatifs aux activités gouvernementales sont des documents à part entière et, à ce titre, doivent être conservés durant une période de temps déterminée ou conservés en permanence, en vertu des politiques et législations en vigueur. Alors que certaines informations doivent être conservées pendant une période de temps minimale, d’autres sont assujetties à des délais de conservation maximaux, à l’expiration desquels elles doivent être éliminées, conformément à la loi.

On estime actuellement, qu’en moyenne, un employé du gouvernement reçoit ou crée au moins 50 courriels par jour, ce qui donne un total de 10 000 courriels par année pour 200 jours ouvrables. Dans le cas d’un ministère comptant 5 000 employés, cela représente plus de 50 millions de courriels par an. Le nombre total d’employés dans la fonction publique a dépassé 350 000 au cours des cinq dernières années; un simple calcul révèle que, dans l’ensemble, les employés du gouvernement pourraient traiter jusqu’à 3 milliards 500 millions de courriels par an. Ce volume de courriels exerce une pression importante sur la capacité de stockage des serveurs, en raison de la quantité de données contenues dans les courriels et les fichiers qui y sont joints. Plus important encore, les courriels sont à l’heure actuelle le principal canal de prise de décision au gouvernement et, pour des fins de reddition de compte, ces documents doivent être gérés avec soin et efficience, afin de garantir qu’ils soient classés et stockés de façon appropriée, et qu’ils puissent être récupérés au besoin, tout au long de leur période de conservation.

0.6. Domaines où les lignes directrices ne s’appliquent pas

Les listes et forums de discussion, ainsi que les listes et calendriers de diffusion constituent des éléments de la gestion des courriels qui ne sont pas abordés dans ces lignes directrices. Cela ne veut pas dire qu’ils ne sont pas importants ou qu’on ne devrait pas s’y intéresser à l’avenir, mais pour l’instant, ces sujets n’ont pas été traités dans la présente version des Lignes directrices pour la gestion des courriels - Feuille de route.

0.7. Feuille de route pour se conformer aux lignes directrices

Le document « Lignes directrices pour la gestion des courriels - Feuille de route » présente l'ensemble de lignes directrices, ainsi qu'une justification et des résultats à atteindre pour chacune d'elles. Chaque institution devra prendre en compte toutes les lignes directrices et recommandations associées; cependant, certaines de ces lignes directrices et recommandations pourront être interprétées à la lumière du mandat et des exigences organisationnelles propres à l'institution.

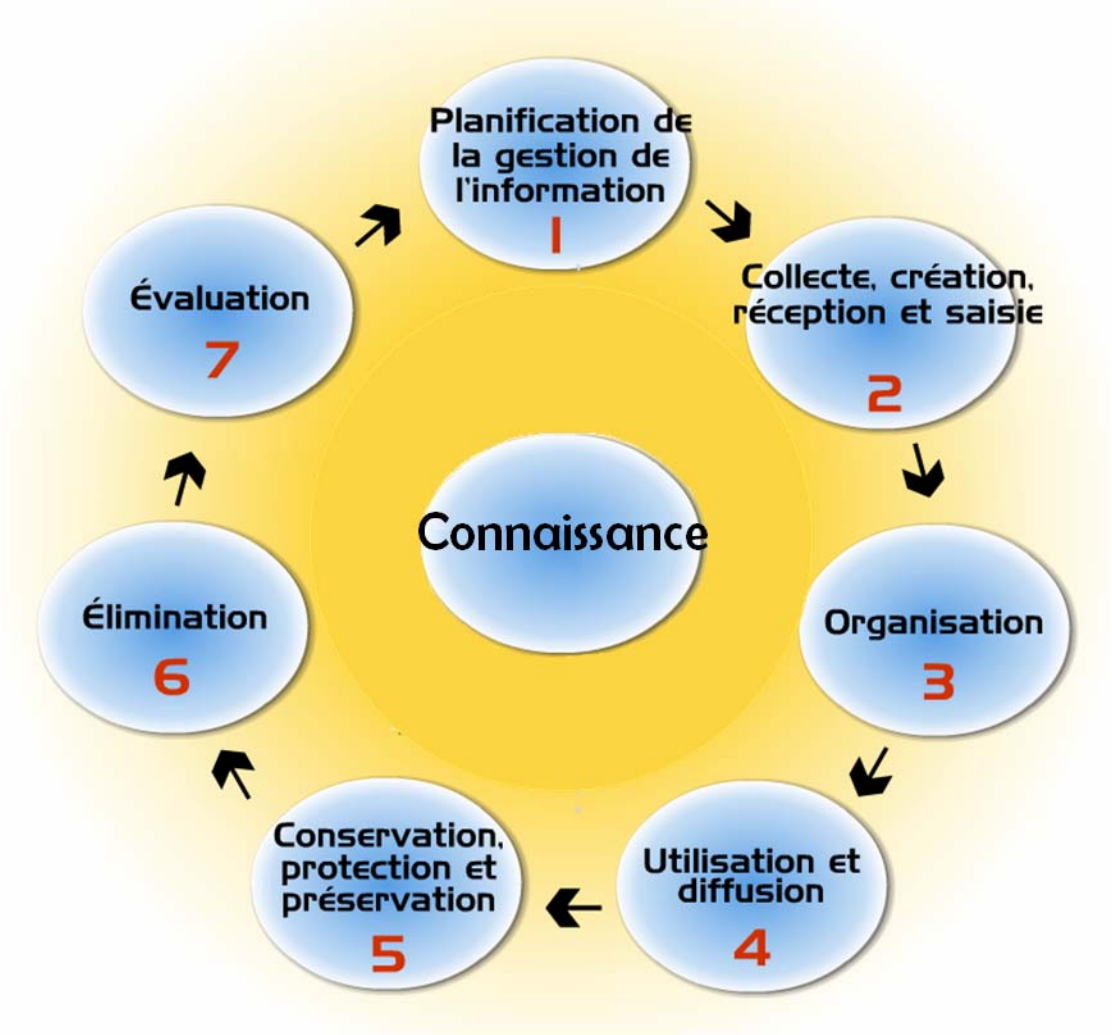
Par conséquent, chacune des lignes directrices et chacune des recommandations devra peut-être être appuyée par une décision et un énoncé de politique de la part de la haute direction de l'institution. La feuille de route a pour objectif de simplifier la rédaction d'une telle politique en proposant un modèle de politique pour chacune des lignes directrices et des actions recommandées. Le texte d'introduction à la politique de gestion des courriels de l'institution devrait indiquer clairement pourquoi l'institution a élaboré une telle politique, et quels seront les bénéfices attendus pour elle-même et ses employés. Vous trouverez ci-dessous un exemple d'introduction.

0.8. Cycle de vie de l'information électronique

Les recommandations contenues dans les présentes lignes directrices pour la gestion des courriels s'articulent autour des sept phases du cycle de vie de l'information électronique.

1. Planification
2. Cueillette, création, réception et saisie
3. Organisation
4. Utilisation et diffusion
5. Maintenance, protection et conservation
6. Élimination
7. Évaluation

Le diagramme qui suit présente le cycle de vie de la gestion de l'information; les sept phases forment le pourtour du cycle. La connaissance qu'une personne a de ses propres responsabilités est cruciale; elle occupe le centre du cycle de vie.



0.9. Définitions

Administrateur de courriel (administrateur de système ou administrateur de réseau)

Personne responsable de la maintenance du système de courriel, incluant toutes les boîtes aux lettres de ce système.

Adresse de courriel

Suite de caractères permettant aux systèmes informatiques de faire parvenir un courriel à son destinataire; cette suite contient habituellement un nom d'utilisateur, le symbole @ et un nom de domaine (par exemple : jsmith@dept-dept.gc.ca).

Authenticité

L'authenticité d'un document réfère à sa fiabilité et son identité au fil du temps. L'authenticité garantit que le document n'a pas été modifié ou manipulé après sa création, sa réception ou sa migration tout au long du processus continu de création, de maintenance et de conservation.

Boîte aux lettres

Zone d'un système informatique où sont stockés les courriels reçus et expédiés par un utilisateur individuel.

Boîte d'envoi

Zone d'un système de courriel où sont stockés les courriels envoyés par un utilisateur. Habituellement, la boîte d'envoi n'est qu'une zone tampon où le courriel est gardé avant d'être envoyé (ce qui, la plupart du temps, se fait presque instantanément). Après l'envoi, une copie du courriel est stockée dans un dossier « Messages envoyés » ou disparaît complètement de la boîte aux lettres de l'expéditeur, selon les règles administratives en vigueur, lesquelles peuvent souvent être personnalisées par l'utilisateur.

Calendrier de conservation

Outil ou document de gestion qui indique les délais de conservation pour tous les documents d'une organisation. Ces délais peuvent varier selon les types de documents.

Compte de courriel

Boîte aux lettres d'un utilisateur et droits d'utilisation de cette boîte.

Copie latente

Lorsqu'un courriel est supprimé, il n'est pas détruit. Il reste sur le disque dur, la bande de sauvegarde ou le serveur tant qu'il n'est pas écrasé par un autre fichier. En fait, lorsqu'un message est « supprimé », c'est uniquement le pointeur électronique vers le message qui est détruit. Selon la capacité du support de stockage électronique, un courriel peut continuer d'exister

sous forme de copie latente pendant plusieurs années avant qu'il ne soit finalement écrasé. Et même à ce moment-là, il sera peut-être encore possible de le récupérer, en tout ou en partie, à l'aide d'une technologie appropriée.

Copie officielle

Ce terme sert à désigner la version d'un document censée être la version originale ou définitive, authentique et fiable à des fins légales.

Courriel

- Système informatique permettant à l'utilisateur de créer, d'expédier, de recevoir, de classer et de répondre à des messages électroniques.
- Message créé, expédié, reçu ou retransmis grâce à réseau électronique.

Courriel non considéré comme un document organisationnel

Aux fins des présentes lignes directrices, n'est pas considéré comme un document organisationnel, tout courriel contenant des informations qui ne sont pas reliées aux activités d'une institution gouvernementale, ou tout type d'information qui n'est pas un document officiel (p. ex., une publication externe, un formulaire vierge ou un manuel d'entretien). Les types de courriels suivants, et les pièces qui y sont jointes, ne sont pas considérés comme des documents organisationnels :

- Correspondance personnelle
- Courriels échangés avec des amis ou des membres de la famille
- Courriels envoyés ou reçus concernant les activités personnelles d'un utilisateur
- Copies d'annonces reçues
- Courriels relatifs à des collectes de sang, des activités de bienfaisance, des événements sociaux ou sportifs auxquels les employés de l'institution sont invités
- Documents publiés par d'autres organismes ou entreprises, accessibles au grand public et qui ne font pas partie d'un document cas ou d'une proposition d'achat
- Catalogues, prospectus ou brochures électroniques
- Journaux, magazines ou livres électroniques
- Matériel promotionnel non sollicité (pourriels)
- Fichiers copiés ou téléchargés à partir de sites Internet

Courrier électronique

Voir « Courriel »

Découverte

La découverte est l'une des étapes d'une action en justice, durant laquelle chacune des parties doit produire toutes les preuves pertinentes au litige en question et qui relèvent de son contrôle. Ceci inclut toute preuve qu'une partie peut utiliser pour défendre son point de vue, ainsi que toute information pouvant être utilisée contre la partie adverse, ou que la partie adverse peut utiliser pour défendre son propre point de vue. En principe, un courriel peut être « découvert » et exigé par la cour aussi longtemps qu'il continue d'exister (voir « Copie latente »).

Délai de conservation

Période de temps durant laquelle un document doit être conservé à des fins administratives, fiscales, juridiques ou historiques.

Document

1. « Éléments d'information, quel qu'en soit le support; la présente définition ne vise pas les publications ». (Loi sur la Bibliothèque et les Archives du Canada, 2004, Loi à jour en date du 13 juin 2008)
2. « Sont assimilés à une pièce l'ensemble ou tout fragment d'un livre, d'un document, d'un écrit, d'une fiche, d'une carte, d'un ruban ou d'une autre chose sur ou dans lesquels des renseignements sont écrits, enregistrés, conservés ou reproduits, et, sauf pour l'application des paragraphes (3) et (4), toute copie ou transcription admise en preuve en vertu du présent article en conformité avec le paragraphe (3) ou (4) ». (Loi sur la preuve au Canada, 1985, Loi à jour en date du 13 juin 2008)
3. « Éléments d'information, quel qu'en soit le support (Loi sur l'accès à l'information, 1985, Loi à jour en date du 13 juin 2008)

Aux fins de ces lignes directrices, un document contient de l'information relative à une transaction effectuée, une décision prise ou une action menée dans le cadre des activités d'une institution gouvernementale, notamment de l'information qui est déterminante (ou considérée comme telle) dans le processus.

Document officiel

Document créé ou reçu dans le cours normal des activités d'une organisation, par exemple, pour effectuer une transaction, fournir un service, prendre une décision ou mener une action

conformément à ses responsabilités et à son niveau d'autorité, en vertu du mandat d'une institution gouvernementale.

Documents essentiels

Certains documents sont essentiels à la poursuite ou au rétablissement des activités vitales de l'institution. Ces sont notamment les documents qui :

- pourraient affecter les droits fondamentaux des personnes et des organisations, tels que les droits légaux, les droits de propriété, etc.;
- sont les plus utilisés et les plus demandés;
- exigeraient un investissement énorme en temps, en argent et en ressources humaines s'ils devaient être reconstitués avec leurs systèmes associés;
- sont similaires à ceux qui ont été inclus par d'autres institutions fédérales dans leur programme de gestion des documents essentiels;
- doivent être conservés en vertu d'une loi ou d'un règlement.

Indexation

Processus par lequel des mots-clés, des expressions et des termes sont utilisés pour faciliter l'identification d'un courriel ou de ses pièces jointes afin de pouvoir le repérer et le récupérer plus tard.

Information ou document éphémère

Les informations éphémères se trouvent dans les documents (éphémères) dont on a besoin seulement pendant une période de temps limitée, afin d'effectuer des activités courantes ou de préparer d'autres documents. Les documents éphémères ne comprennent pas les documents ayant une valeur historique, ni les documents nécessaires aux institutions fédérales ou aux ministres pour contrôler, appuyer ou documenter la réalisation de programmes, pour effectuer des opérations, prendre des décisions, ou rendre compte des activités du gouvernement.

Voici quelques exemples d'informations éphémères que l'on retrouve dans les courriels :

- Nouvelles diffusées via divers médias par voie de courriel ou de communiqués internes, par exemple
- Communiqués
- Avis à l'ensemble du personnel, annonces d'événements spéciaux
- Demandes relatives à la tenue d'une réunion
- Offres de formation

- Invitations
- Messages personnels
- Photos en format JPEG, GIF, ou autre
- Messages à titre informatif (PVI – pour votre information)
- Annonces, journaux, livres, brochures, bulletins ou rapports publiés en format électronique
- Courriels imprimés sur papier ou saisis dans un système de classement électronique
- Demandes d'information de routine
- Avis (départ en vacances, campagnes de sollicitation, etc.)
- Anciennes versions de documents de travail

Intégrité

L'intégrité fait référence à la fiabilité et à la fidélité des documents, qu'il s'agisse d'originaux, de reproductions ou de représentations comparables de documents électroniques. L'intégrité fait aussi référence à la fiabilité et à la fidélité du système de gestion des documents dans lequel les documents électroniques sont enregistrés ou stockés pour produire des copies et des duplicatas fiables et fidèles de ces documents.

Lignes directrices pour la gestion des courriels

Les lignes directrices pour la gestion des courriels sont des règles, des pratiques et des exigences mesurables qui servent de modèle pour la gestion des courriels, de leurs métadonnées et pièces jointes.

Liste de diffusion

Liste d'adresses électroniques servant à envoyer des courriels à plusieurs personnes à la fois.

Loi et règlements sur l'AIPRP et demande d'accès en vertu de l'AIPRP

Le sigle AIPRP désigne l'accès à l'information et la protection des renseignements personnels; il est souvent employé pour identifier les demandes d'accès formulées en vertu de cette législation. L'accès à l'information est le principe général selon lequel les Canadiens peuvent demander à consulter des dossiers du gouvernement fédéral. Cet accès est parfois restreint, par exemple dans le cas où l'information demandée contient des renseignements personnels sur un individu (autre que celui qui fait la demande).

Mémoire institutionnelle - documents

Documents officiels découlant des fonctions et activités d'une institution gouvernementale, en vertu de son mandat, de son encadrement législatif, et des programmes et services qu'elle offre. Ces documents, qui constituent la mémoire institutionnelle, peuvent être créés ou utilisés à diverses fins.

- Offrir différents programmes et services
- Documenter des activités financières ou administratives
- Traiter diverses questions d'ordre juridique
- Prendre ou documenter des décisions ayant des impacts sur les politiques, les programmes ou les procédures
- Rendre compte au Parlement
- Saisir et documenter des événements qui pourraient avoir une certaine importance historique
- Documenter le pourquoi et le comment des décisions prises ou des actions menées

Les documents constituant la mémoire institutionnelle sont soumis à des calendriers de conservation approuvés par l'organisme et par Bibliothèque et Archives Canada, et doivent être gérés par des systèmes officiels de gestion des documents. Ces documents ne peuvent être détruits sans une autorisation de disposition de documents émise par Bibliothèque et Archives Canada.

Mémoire institutionnelle - information

La mémoire institutionnelle se retrouve dans les documents officiels et les souvenirs que certaines personnes peuvent avoir conservé des activités de leur organisation, mais elle se trouve aussi sur divers formats et supports électroniques qui gardent la trace des opérations courantes et des processus décisionnels. Ces informations constituent des ressources importantes pour l'organisation, car elles représentent l'expérience, le savoir et la mémoire des individus qui y ont travaillé. La mémoire institutionnelle fournit les bases nécessaires pour prendre de bonnes décisions, et témoigne des raisons justifiant ces décisions, incluant les circonstances, le contexte et d'autres renseignements disponibles lors de la prise de décision. Le courriel est devenu une très

importante source de mémoire institutionnelle, même si, à ce jour, son plein potentiel a rarement été exploité de manière efficiente et organisée.

Message courriel

Document créé, transmis, reçu ou transféré dans un système électronique de courrier.

Métadonnées

Informations décrivant un ensemble de données (p. ex. : objet, date et destinataire d'un courriel).

Mot de passe

Chaîne de caractères habituellement choisie par un utilisateur, reconnaissable par le système informatique et utilisée en association avec un nom d'utilisateur, pour identifier et authentifier cet utilisateur et lui autoriser l'accès au système.

Serveur de courriel

Ordinateur en réseau qui fournit des services de courriel à d'autres ordinateurs de ce réseau.

Système de courriel

Système informatique comprenant des ordinateurs et des logiciels, utilisé essentiellement à des fins de communication; les utilisateurs peuvent créer, transmettre, recevoir, classer et répondre à des messages de manière électronique.

Un système de courriel n'est pas un système de gestion des documents et ne convient pas pour classifier, classer et stocker des messages électroniques (voir : Système de gestion des documents).

Plusieurs systèmes de courriel offrent aussi une fonctionnalité de calendrier, grâce à laquelle les utilisateurs peuvent fixer la date d'une réunion, réserver une salle ou de l'équipement, envoyer, accepter ou refuser une invitation. De plus, les systèmes de courriel permettent souvent aux utilisateurs de créer des listes de tâches à effectuer et de leur attribuer un ordre de priorité; certains sont même couplés à un système de messagerie sans fil ou de messagerie vocale. Les systèmes de courriel évoluent très rapidement.

Système de gestion de l'information

Travaux publics et Services gouvernementaux Canada (TPSGC) définit son système de gestion des dossiers, des documents et de l'information (SGDDI) comme « … une suite d'applications conçue pour doter les ministères et organismes du gouvernement fédéral d'un logiciel économique de gestion des dossiers et des documents ».

(Source : http://www.tpsgc.gc.ca/rdims/text/index-f.html)

Système de gestion des documents

Un système de gestion des documents est un dépôt à long terme et des processus associés permettant d'entreposer, de conserver, de consulter et, finalement, d'éliminer des documents organisationnels d'une institution. Un tel système s'appuie sur des méthodes et des technologies pour l'entreposage des documents, tant sur support papier qu'en format électronique.

Threading

Mécanisme par lequel un système de gestion de l'information peut suivre à la trace les relations existant entre des courriels, leurs métadonnées et pièces jointes, à l'intérieur d'une suite de courriels.

1. Les institutions doivent se doter d'un plan pour gérer les courriels

Depuis une dizaine d'années, la gestion des courriels constitue l'un des plus importants défis à relever en gestion de l'information. Les organisations devront concevoir des plans d'ensemble détaillés, afin d'arriver à maîtriser la croissance phénoménale de ce moyen de communication électronique, avec sa gamme de plus en plus large d'utilisations, de caractéristiques et de fonctionnalités.

Le plan doit incorporer plusieurs composantes de la gestion des courriels, notamment :

- l'élaboration de politiques et procédures relatives à la gestion des courriels, en lien avec les activités de l'institution;
- une gestion intégrée des avantages et inconvénients du courriel, qui accordera une égale importance aux messages électroniques, à leurs métadonnées et pièces jointes, et permettra l'utilisation d'infrastructures communes et l'interopérabilité des systèmes de courriel et de gestion de l'information;
- la prise en compte, dès le départ, des exigences propres à la gestion des courriels lors de l'élaboration de nouveaux programmes, politiques, services et systèmes fondés sur la technologie;
- la mise en place de structures de gouvernance et de responsabilisation pour la gestion de l'information en général, et des courriels en particulier;
- des programmes de sensibilisation et de formation sous diverses formes.

Résultats attendus

Toutes les institutions du gouvernement fédéral auront obtenu les résultats suivants.

- Un plan détaillé de gestion des courriels sera appuyé et adéquatement financé par la haute direction.
- Le plan de gestion des courriels indiquera de quelle manière les Lignes directrices pour la gestion des courriels au gouvernement du Canada seront respectées.
- Chacune des recommandations relatives à la gestion des courriels sera considérée attentivement.
  - Si recommandation est adoptée, il en sera fait mention.
  - Si une recommandation doit être interprétée à la lumière du mandat de l'institution ou de son champ d'activités, cette interprétation sera fournie.

- Si une recommandation doit être adaptée au mandat de l'institution ou à son champ d'activités, la nature de cette adaptation sera indiquée.
- Si une recommandation ne s'applique pas, on en donnera la raison ou on proposera une autre recommandation.

1.1. Gérer les programmes et les systèmes de courriel de manière intégrée

Tous les programmes de courriel utilisés par les institutions, et les systèmes qui leur sont associés, devraient être financés adéquatement par la direction; ils devraient aussi être conçus et configurés de façon à leur permettre de saisir, stocker et gérer efficacement les courriels reçus et expédiés, avec leurs métadonnées et leurs pièces jointes.

Une sélection de courriels contenant des informations et des documents gouvernementaux devrait être extraite du reste des documents moins pertinents et conservée pendant une durée de temps appropriée, conformément au cycle de vie de la gestion de l'information recommandé dans la Politique sur la gestion de l'information.

Note : Dans le tableau ci-dessous, la cellule claire indique à qui appartient la responsabilité de mettre en oeuvre ou d'appliquer la recommandation.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

1.2. Offrir des programmes de sensibilisation et de formation à la gestion des courriels

Des programmes de sensibilisation et de formation à la gestion des courriels devraient être mis sur pied afin d'aider les employés à développer les connaissances et habiletés qui leur permettront d'utiliser le courriel de manière efficace et appropriée.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

1.3. Utiliser divers supports pour sensibiliser et former à la gestion des courriels

Divers supports devront être utilisés afin que les Lignes directrices pour la gestion des courriels, ainsi que les politiques et les procédures associées soient bien comprises et mises en œuvre dans l'organisation.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

1.4. Vérifier que les Lignes directrices pour la gestion des courriels, ainsi que les politiques et procédures associées, ont été bien distribuées, lues et comprises

Chaque institution devra distribuer les Lignes directrices pour la gestion des courriels, ainsi que les politiques et procédures associées, afin que les dispositions contenues dans ces documents soient bien connues et comprises de tous ses employés, contractuels et autres utilisateurs relevant de son autorité.

L'institution devra également informer ses employés, contractuels et autres utilisateurs qu'elle attend d'eux qu'ils se conforment aux Lignes directrices pour la gestion des courriels et à toutes les recommandations adoptées par l'institution, et qu'un usage abusif du système de courriel peut entraîner des mesures disciplinaires pouvant aller jusqu'au congédiement ou à la résiliation d'un contrat.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

1.5. Conserver des dossiers sur les activités de formation et sur la participation

Les institutions devraient conserver des dossiers sur les activités de formation en gestion des courriels, ainsi que sur l'assistance à tout atelier, cours en classe ou présentation sur le sujet. Ces dossiers devraient être conservés pendant une longue période de temps afin de pouvoir être consultés, au besoin, dans le cadre d'un audit ou d'une action en justice.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

2. Les institutions doivent recueillir et conserver tous les courriels relatifs à leurs activités organisationnelles

Conformément à la Politique sur la gestion de l'information, les institutions sont tenues de recueillir, créer, recevoir et conserver tous les courriels relatifs à leurs activités organisationnelles, notamment les courriels contenant des informations constitutives de la mémoire institutionnelle et des données servant à prendre une décision ou à entreprendre une action visant à :

- soutenir la prestation de services, l'élaboration de politiques judicieuses et la prise de décisions éclairée, et répondre aux exigences organisationnelles, juridiques et de reddition de comptes;
- assurer la pertinence, la fiabilité et l'exhaustivité de l'information;
- optimiser le partage et la réutilisation de l'information conformément aux obligations découlant des lois et des politiques;
- documenter les décisions et les processus décisionnels pour rendre compte des activités du gouvernement, reconstituer l'évolution des politiques et des programmes, assurer la continuité du gouvernement et de son processus décisionnel, et permettre une vérification et un examen indépendants;
- réduire le fardeau des réponses aux demandes d'accès à l'information et aux demandes de preuves légales en évitant la collecte inutile de renseignements.

La gestion de tous ces documents soulève des questions fondamentales, notamment, combien d'exemplaires d'un document devrait-on conserver. Plus il y a d'exemplaires d'un même document, plus il y a d'endroits où ils peuvent se trouver, et plus il est difficile de les gérer. Afin de faciliter l'étape suivante du cycle de vie des documents (l'organisation), il est très important de conserver les métadonnées, c'est-à-dire les informations relatives aux courriels. Ces métadonnées peuvent comprendre le nom de l'expéditeur et le nom des destinataires, la date d'envoi du courriel, sa date de réception, l'objet du message et plusieurs autres informations pouvant servir à classer et à repérer le courriel ultérieurement.

Résultats attendus

Toutes les institutions du gouvernement fédéral auront obtenu les résultats suivants :

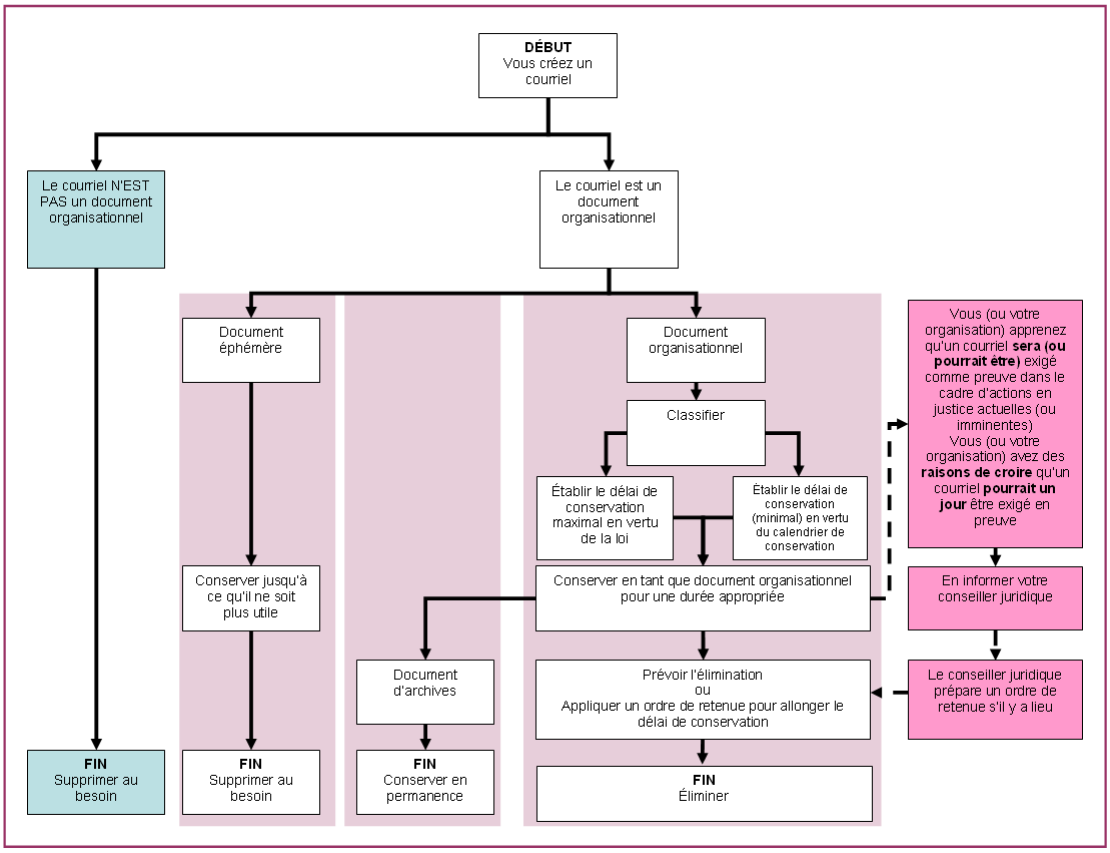
- Tous les utilisateurs du courriel vont créer, expédier, recevoir, réacheminer et stocker leurs courriels conformément aux présentes Lignes directrices pour la gestion des courriels, et à toutes les recommandations applicables.

- Les employés sauront quels messages conserver ou éliminer, et se chargeront de gérer leurs propres boîtes aux lettres et leurs propres dossiers sur une base régulière.
- Un seul exemplaire d'un courriel sera conservé, dans un dépôt autorisé, où il aura le statut de « copie officielle ».
- Les pièces jointes seront stockées avec le message ou, sinon, seront liées au message de manière fiable.
- Les métadonnées associées aux courriels seront conservées.

2.1. Créer, expédier et stocker les courriels de manière structurée

Tout message contenant de l'information utilisée dans (ou considérée dans, ou concernant) une transaction effectuée, une décision prise ou une action entreprise dans le cadre des activités organisationnelles d'une institution gouvernementale doit être conservé.

Le diagramme suivant illustre le processus recommandé pour créer, expédier et stocker les courriels au gouvernement du Canada.

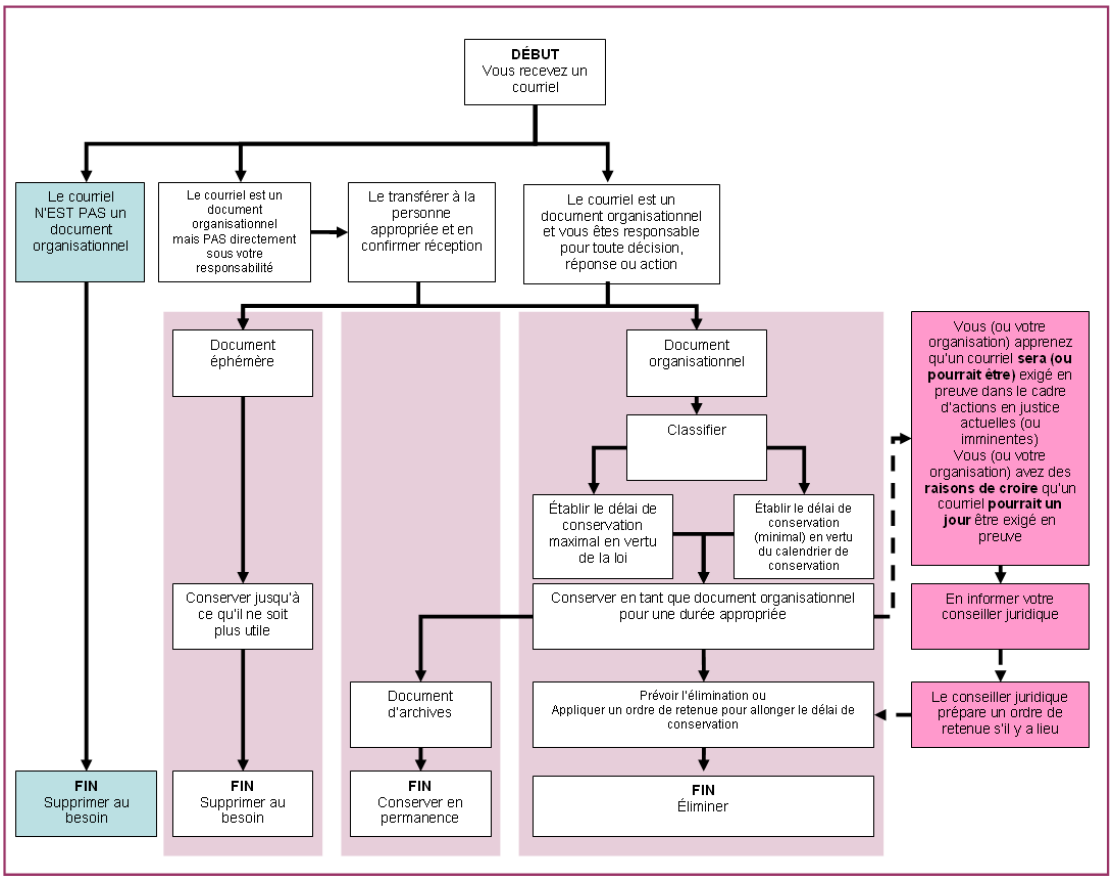

DÉBUT
Vous créez un courriel
Le courriel N'EST PAS un document organisationnel
Le courriel est un document organisationnel
Document éphémère
Document organisationnel
Classifier
Établir le délai de conservation maximal en vertu de la loi
Établir le délai de conservation (minimal) en vertu du calendrier de conservation
Vous (ou votre organisation) apprenez qu'un courriel sera (ou pourrait être) exigé comme preuve dans le cadre d'actions en justice actuelles (ou imminentes)
Vous (ou votre organisation) avez des raisons de croire qu'un courriel pourrait un jour être exigé en preuve
Conserver jusqu'à ce qu'il ne soit plus utile
Conserver en tant que document organisationnel pour une durée appropriée
En informer votre conseiller juridique
Document d'archives
Prévoir l'élimination
ou
Appliquer un ordre de retenue pour allonger le délai de conservation
Le conseiller juridique prépare un ordre de retenue s'il y a lieu
FIN
Supprimer au besoin
FIN
Supprimer au besoin
FIN
Conserver en permanence
FIN
Éliminer

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

2.2. Recevoir et stocker les courriels de manière structurée

Tout message reçu, contenant de l'information utilisée dans (ou considérée dans, ou concernant) une transaction effectuée, une décision prise ou une action entreprise dans le cadre des activités organisationnelles d'une institution gouvernementale doit être conservé.

Le diagramme suivant illustre le processus recommandé pour recevoir et stocker les courriels dans les institutions.


DÉBUT
Vous recevez un courriel
Le courriel N'EST PAS un document organisationnel
Le courriel est un document organisationnel mais PAS directement sous votre responsabilité
Le transférer à la personne appropriée et en confirmer réception
Le courriel est un document organisationnel et vous êtes responsable pour toute décision, réponse ou action
Document éphémère
Conserver jusqu'à ce qu'il ne soit plus utile
FIN
Supprimer au besoin
FIN
Supprimer au besoin
Document d'archives
FIN
Conserver en permanence
Document organisationnel
Classifier
Établir le délai de conservation maximal en vertu de la loi
Établir le délai de conservation (minimal) en vertu du calendrier de conservation
Conserver en tant que document organisationnel pour une durée appropriée
Prévoir l'élimination ou
Appliquer un ordre de retenue pour allonger le délai de conservation
FIN
Éliminer
Vous (ou votre organisation) apprenez qu'un courriel sera (ou pourrait être) exigé en preuve dans le cadre d'actions en justice actuelles (ou imminentes)
Vous (ou votre organisation) avez des raisons de croire qu'un courriel pourrait un jour être exigé en preuve
En informer votre conseiller juridique
Le conseiller juridique prépare un ordre de retenue s'il y a lieu

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

2.3. Gérer les boîtes aux lettres et les dossiers individuels sur une base régulière

Pour gérer les boîtes aux lettres (boîtes de réception, messages envoyés, messages supprimés), les courriels devraient être régulièrement classifiés et placés dans un dossier approprié. Les courriels éphémères peuvent être placés dans la corbeille (messages supprimés).

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

2.4. Garder un seul exemplaire de chaque courriel

Dans la mesure du possible, les organisations ne devraient conserver, à titre de document officiel, qu'un seul exemplaire d'un courriel (outre la copie de sécurité), avec ses métadonnées et pièces jointes, dans un dépôt qu'elles gèrent ou contrôlent. Le logiciel de courriel lui-même doit être considéré comme un dispositif de communication et non de stockage. Les courriels devraient être transférés le plus rapidement possible dans un dépôt de documents indépendant. Puisque toute copie d'un courriel conservée peut être recherchée dans le cadre d'une action en justice, aucune autre copie de ce courriel ne devrait être conservée dans un autre dépôt ou par un individu dans l'organisation. La fonction « supprimer » élimine le pointeur électronique vers un courriel, mais ne détruit pas le message lui-même. Le message continue d'exister tant qu'il n'est pas écrasé par de nouvelles données.

Par exemple, un courriel ne devrait pas être conservé sur le disque dur d'un utilisateur. Une copie d'un courriel pourrait toutefois être stockée temporairement sur une clé USB ou sur le disque dur d'un ordinateur portatif aux fins d'une présentation, mais elle devrait être effacée de manière sécuritaire après la présentation.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

2.5. Gérer et conserver les pièces jointes aux courriels

Aux fins des présentes Lignes directrices pour la gestion des courriels, un système de gestion des courriels devrait conserver ensemble, dans le même dépôt, un message et sa ou ses pièces jointes, et être en mesure de prouver de manière fiable la relation existant entre ces documents.

Un système de gestion des courriels pourrait, aussi, conserver un message et ses pièces jointes dans des dépôts séparés, pourvu qu'il puisse fournir une preuve fiable qu'ils sont interreliés.

Les pièces jointes doivent être dans un format électronique pouvant être rattaché à un courriel : enregistrement audio, vidéo, message vocal, carte, graphique, photo numérique, feuille de calcul, base de données, présentation, texte, etc.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

2.6. Considérer les courriels comme des biens, soumis au contrôle juridique du gouvernement du Canada

Les employés et les contractuels qui utilisent le système de courriel d'une institution fédérale devraient être informés que les courriels qu'ils créent, expédient ou reçoivent grâce à ce système ne leur appartiennent pas, que ces courriels peuvent être surveillés par l'institution et qu'ils ne devraient pas être considérés comme des messages personnels, de nature privée.

Tous les courriels, métadonnées et pièces jointes créés, reçus ou conservés par un système de courriel, une bande de sauvegarde, un serveur ou un autre moyen de stockage sous le contrôle d'une institution fédérale (incluant les ordinateurs portatifs, les clés USB, les CD et autres moyens de stockage portatifs) sont considérés comme la propriété de l'institution et devraient être traités comme tels.

Tout courriel créé, expédié ou reçu par un employé utilisant le système de courriel d'une institution fédérale est considéré comme étant sous le contrôle et la propriété de l'institution, peu importe l'endroit où il est conservé.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes de la gestion de l'information	Gestionnaires des opérations	Dirigeants

2.7. Utiliser avec modération les listes de diffusion institutionnelles

Les listes de diffusion destinées à l'ensemble de l'institution, ses directions, bureaux, divisions, etc. ne devraient être utilisées que par des personnes autorisées, à des fins officielles approuvées par la haute direction.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

2.8. Fournir un bloc-signature et les coordonnées de la personne-ressource

Conformément à la politique de normalisation des sites internet du gouvernement du Canada (http://www.tbs-sct.gc.ca/clf2-nsi2/index-fra.asp), tous les courriels envoyés par les employés du gouvernement doivent indiquer le nom de l'expéditeur, le nom de son institution, ses numéros de téléphone et de télécopieur avec l'indicatif régional et le numéro du poste, ainsi que son adresse postale et son adresse de courriel. Tous les courriels envoyés par les employés du gouvernement doivent afficher de manière uniforme le mot-symbole « Canada » et la signature institutionnelle.

Certaines exemptions ou exceptions sont autorisées lorsque l'expéditeur a des motifs valables de vouloir préserver la confidentialité de ses messages, ou pour des raisons de sécurité personnelle, matérielle ou nationale.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

2.9. Ajouter un avis de confidentialité ou de non-responsabilité, s'il y a lieu

Les institutions doivent se demander s'il est approprié à leur situation d'insérer un avis de confidentialité ou de non-responsabilité sous le bloc-signature. En réfléchissant à cette question, l'organisme devrait procéder à une analyse de risque afin d'établir s'il est possible de limiter sa responsabilité. Voici un exemple d'un tel avis.

Avis de non-responsabilité
Ce courriel, incluant toute pièce jointe, s'adresse exclusivement à son destinataire et peut contenir des informations confidentielles ou privilégiées. (Nom de l'institution) ne peut être tenu responsable pour toute perte ou dommage subi par une personne, en raison d'une utilisation non autorisée de ce courriel ou parce qu'elle s'est fiée à l'information contenue dans ce courriel. Si vous n'êtes pas le destinataire prévu, nous vous avisons, par la présente, que toute diffusion, reproduction ou autre utilisation de ce courriel est strictement interdite. Veuillez nous signaler toute erreur de communication par retour du courrier et détruire tous les exemplaires de ce courriel. Merci.

La décision d'inclure ou non un tel avis de non-responsabilité (et la formulation exacte de cet avis) relève des dirigeants de l'institution, en consultation avec leurs conseillers juridiques.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

2.10. Ajouter un avis d'opinion personnelle, s'il y a lieu

Les institutions doivent examiner s'il est approprié à leur situation de demander aux utilisateurs d'insérer un avis d'opinion personnelle, dans certaines circonstances. Voici un exemple d'un tel avis.

Avis d'opinion personnelle
Ce courriel, incluant toutes les pièces jointes, reflète l'opinion personnelle de l'expéditeur et ne représente pas l'opinion ou la position officielle de (nom de l'institution). (Nom de l'institution) ne peut être tenu responsable pour toute perte ou dommage subi par une personne, en raison d'une utilisation non autorisée de ce courriel ou parce qu'elle s'est fiée à l'information contenue dans ce courriel. Si vous n'êtes pas le destinataire prévu, nous vous avisons, par la présente, que toute diffusion, reproduction ou autre utilisation de ce courriel est strictement interdite. Veuillez nous signaler toute erreur de communication par retour du

Avis d'opinion personnelle
courrier et détruire tous les exemplaires de ce courriel. Merci.

La décision d'inclure ou non un tel avis d'opinion personnelle (et la formulation exacte de cet avis) relève des dirigeants de l'institution, en consultation avec leurs conseillers juridiques.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes de la gestion de l'information	Gestionnaires des opérations	Dirigeants

2.11. Éviter d'utiliser la fonction « Répondre à tous »

Les utilisateurs qui reçoivent un courriel adressé à plusieurs personnes, ou en tant que membre d'une liste de diffusion, devraient éviter d'employer la fonction « Répondre à tous », sauf si la réponse présente un réel intérêt pour la majorité des personnes ayant reçu le message original.

Un des risques liés à l'utilisation de la fonction « Répondre à tous » est qu'en raison de la large diffusion du message, il peut être difficile de savoir exactement à qui revient la responsabilité d'agir.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

3. Les institutions doivent classer les courriels relatifs à leurs activités selon un plan de classification basé sur leurs exigences organisationnelles

La gestion des courriels exige l'établissement d'une méthode de description de l'information institutionnelle qui soit coordonnée et couvre l'ensemble des documents. Afin d'éviter une accumulation de courriels difficile à gérer, tous les messages et leurs pièces jointes, destinés à être conservés durant une période déterminée, doivent être bien classés, au moment opportun, selon un plan de classification à jour et global. Les boîtes aux lettres individuelles, les boîtes communes et les boîtes publiques devraient être gérées efficacement et de manière uniforme. La ligne « Objet » des courriels est souvent utilisée comme outil de recherche et doit donc refléter le plus fidèlement possible le contenu du message. Le système de classement des courriels devrait favoriser l'indexation, le stockage et la récupération des messages de manière structurée et efficace. Le système de classement devrait également préserver tout lien ou fil conducteur entre les courriels à l'intérieur d'une série, afin de pouvoir mettre en contexte chacun des messages.

Résultats attendus

Toutes les institutions du gouvernement fédéral auront obtenu les résultats suivants.

- Il y aura une description détaillée des documents de l'institution.
- Il y aura un ou des plans de classification détaillés et à jour, qui incluront les métadonnées.
- Les utilisateurs sauront où classer leurs courriels, ou ils seront guidés par des systèmes automatisés pour choisir l'endroit approprié.
- Les utilisateurs connaîtront et mettront en pratique des techniques simples pour faciliter la recherche et la récupération des documents.

3.1. Maintenir et utiliser un système structuré et efficace de classement des courriels

Les courriels, à l'exception des messages éphémères et de ceux qui ne sont pas des documents organisationnels, devraient être retirés du système de courriel et placés dans un système séparé où ils seront classés selon un plan de classification approuvé par l'institution. Les courriels devraient être indexés et conservés pour être utilisés par l'institution, jusqu'au moment de leur élimination prévue au calendrier de conservation ou de leur archivage permanent. Le dépôt d'archives devra aussi être structuré et indexé pour assurer un repérage efficace.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

3.2. Déterminer où classer la copie « officielle »

Un plan de classification et un dépôt devraient être établis pour stocker les courriels reçus et envoyés qui sont considérés comme des documents gouvernementaux ou de l'information gouvernementale.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

3.3. Conserver les métadonnées associées aux courriels

Les métadonnées associées à un courriel devraient être conservées, tel que spécifié dans le document NCTTI 39 : Normes de l'information et de la technologie du Conseil du Trésor.

- Partie 1: Norme des métadonnées du Gouvernement en direct

(Source : http://www.tbs-sct.gc.ca/its-nit/standards/tbits39/crit391_fra.asp)

- Partie 2 : Norme du vocabulaire contrôlé

(Source : http://www.tbs-sct.gc.ca/cio-dpi/pols_fra.asp#IT)

La norme NCTTI 39 - Partie 1 – Norme des métadonnées du Gouvernement en direct, a adopté le *Dublin Core*, tel que décrit à l'adresse http://www.dublincore.org/ comme principale norme de métadonnées pour la découverte des ressources. Les métadonnées sont essentielles pour atteindre les objectifs de navigation, de recherche, de partage de l'information et d'interopérabilité du Gouvernement en direct.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

3.4. Classifier et classer les courriels systématiquement et fréquemment

Les courriels devraient être classifiés et classés systématiquement et régulièrement, à une fréquence qui convient à la nature des activités de l'institution (p. ex., une fois par jour), et conformément au plan de classification adopté par l'institution. Les courriels devraient ensuite être transférés dans un dépôt de données désigné par l'institution.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

3.5. Gérer le stockage en ligne temporaire des courriels

Un système de courriel devrait être en mesure de traiter les messages reçus et envoyés, leurs métadonnées et pièces jointes, et de les stocker temporairement en ligne (dans le système lui-même), jusqu'à ce qu'ils soient supprimés ou déplacés manuellement. Les dossiers devraient ensuite être rangés, à intervalles appropriés, dans une zone de stockage de longue durée, par l'utilisateur ou l'administrateur de système, ou grâce à un quelconque mécanisme automatisé.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

3.6. Utiliser à une seule fin les boîtes aux lettres communes ou publiques et les dossiers de courriels

Une boîte aux lettres commune ne devrait être créée qu'à une seule fin et n'avoir qu'un seul propriétaire, lequel fixera des règles bien précises à l'intention des autres personnes qui y ont accès.

Les courriels qui ne correspondent pas à l'objectif de la boîte aux lettres ne devraient pas y être stockés. Il peut s'avérer nécessaire d'attribuer différents niveaux d'accès aux utilisateurs d'une boîte aux lettres commune ou d'un dossier, selon leur rôle ou leur responsabilité.

Les boîtes aux lettres publiques ne devraient être utilisées qu'à une seule fin ou à une fin restreinte et devraient être gérées par un seul propriétaire qui en établit les règles d'accès.

Les boîtes aux lettres individuelles peuvent aussi être mises en commun, jusqu'à un certain point, avec un nombre restreint de personnes faisant partie du groupe de travail de l'utilisateur.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

3.7. Limiter le contenu des courriels à un seul sujet

Les utilisateurs ne devraient traiter que d'un seul sujet par courriel.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

3.8. Décrire l'objet d'un courriel en termes clairs et significatifs

Les utilisateurs devraient décrire l'objet de leurs courriels en termes significatifs, à l'aide de mots clés pouvant servir lors d'une recherche électronique.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

3.9. Prévoir un système d'indexation des courriels

Les institutions devraient prévoir une indexation des courriels.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

3.10. Prévoir un mécanisme permettant de suivre le fil conducteur reliant les courriels entre eux (*threading*)

Les institutions devraient pouvoir suivre le fil conducteur qui relie les courriels entre eux. Le *threading* est un mécanisme par lequel un système de gestion de l'information peut suivre à la trace les relations existant entre des courriels, leurs métadonnées et pièces jointes, à l'intérieur d'une suite de courriels.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

4. Les institutions doivent veiller à ce que l'utilisation du courriel contribue à la réalisation d'activités correspondant à leurs objectifs organisationnels

L’utilisation du courriel devrait être réservée à des usages appropriés et non à la transmission d’informations sensibles, protégées ou secrètes. Les journaux d’exploitation permettent de suivre à la trace l’utilisation des courriels et de préparer des rapports en conséquence, ceci afin de documenter le respect des politiques et procédures en vigueur, tant au niveau individuel que collectif. Le courriel est devenu une des formes de preuve les plus fréquemment utilisées par les tribunaux; les institutions doivent donc, en tout temps, être en mesure de communiquer des preuves sous forme de courriel. La gestion des courriels doit permettre aux utilisateurs un accès pratique et au moment opportun à des informations contenues dans les courriels, conformément aux exigences légales et règlementaires. Il pourrait être instructif d’utiliser des cas réels ou fictifs pour éprouver et analyser la capacité de l’organisme à repérer et à produire des courriels en preuve, de manière fiable et économique, lorsqu’ils sont requis par un tribunal, lors d’un audit ou d’une demande d’accès à l’information en vertu de l’AIPRP.

Résultats attendus

Toutes les institutions du gouvernement fédéral auront obtenu les résultats suivants :

- Les utilisateurs auront accès, de manière pratique et en temps opportun, aux informations qu’ils sont autorisés à voir ou à utiliser, et sauront comment procéder.
- Les cas réels exigeant le repérage de courriels à des fins juridiques, d’audit ou de demande d’information en vertu de l’AIPRP seront surveillés et analysés de manière régulière, afin d’établir des critères de performance, d’évaluer les risques et d’identifier les améliorations à apporter à la gestion des courriels.
- Des « exercices de découverte » à partir de cas fictifs seront conçus et menés occasionnellement afin de diagnostiquer de manière contrôlée la capacité de l’organisme à repérer et à produire des courriels.
- Les leçons apprises au cours de ces exercices seront partagées et mises en pratique.

4.1. Ne pas utiliser le courriel pour traiter de sujets sensibles, personnels, protégés ou secrets, sauf dans les cas autorisés et en respectant les normes de sécurité en vigueur

Il faut éviter d'utiliser le courriel pour transmettre des informations confidentielles, sensibles, protégées ou secrètes, sauf s'il existe une raison opérationnelle précise de le faire et s'il est possible de recourir à des systèmes sécurisés ou au chiffrement des données. Le cas échéant, les utilisateurs doivent se conformer aux politiques et lignes directrices institutionnelles et gouvernementales en la matière (voir aussi 5.1.5).

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

4.2. Utiliser les journaux d'exploitation pour créer une piste de vérification et veiller au respect des règles

Les journaux d'exploitation devraient être utilisés pour créer une piste de vérification enregistrer chacune des opérations effectuées en rapport avec les courriels, dans un système de courriel ou autre dépôt de données.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

4.3. Afficher les noms dans les en-têtes et les adresses de courriel

L'en-tête d'un courriel devrait afficher le nom de l'auteur (De) et celui du destinataire (À), conformément aux normes gouvernementales relatives aux métadonnées.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

4.4. Être prêt à divulguer un courriel en preuve, sous forme électronique

Les systèmes de stockage et de classement des courriels, incluant les systèmes en ligne et les systèmes de stockage de proximité, qu'ils soient à court ou à long terme, doivent permettre aux chercheurs d'identifier, de divulguer ou de produire rapidement des courriels, ainsi que leurs métadonnées et pièces jointes, lors d'une action en justice, d'un audit ou d'une demande en vertu de l'AIPRP. Afin de faciliter la récupération efficiente d'un document à des fins de divulgation, les courriels devraient être classés conformément à un plan de classification institutionnel approuvé (voir aussi la troisième section des Lignes directrices et les recommandations qui s'y trouvent).

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

4.5. Surveiller la performance des activités de découverte et de disposition des courriels

Les organismes devraient surveiller l'efficacité de leur performance en matière de découverte et de disposition des courriels. Ceci est nécessaire en vertu de plusieurs politiques du Secrétariat du Conseil du trésor, notamment la Politique sur la gestion de l'information, la Politique sur la surveillance active, la Politique d'évaluation et la Politique sur la vérification interne.

Des « exercices » devraient être menés régulièrement, que ce soit à partir de cas réels ou de cas simulés pour l'occasion. On en profitera alors pour concevoir et tester des mesures de

performance, et évaluer l'efficience et l'efficacité des procédures de découverte et de disposition des courriels.

Les observations résultant de ces exercices devraient être partagées et analysées sous forme de « leçons apprises », et mises à la disposition de toute personne impliquée dans la découverte ou la disposition des courriels, ou dans l'évaluation et l'amélioration des pratiques de l'institution en matière de gestion de l'information.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

5. Les institutions doivent veiller à ce que leurs courriels soient maintenus, protégés et conservés selon des calendriers de conservation appropriés

Les institutions doivent veiller à ce que l'information possédant une valeur de conservation permanente pour le gouvernement du Canada ou pour les Canadiens puisse être utilisée, maintenant et dans les années futures. Les institutions devraient effectuer une évaluation des risques afin d'établir les délais de conservation appropriés à chaque type d'information. L'établissement de ces délais repose essentiellement sur le contenu des documents et non sur leur support physique ou sur la technologie utilisée pour les créer. Les utilisateurs du courriel devraient se référer au plan de classification et au calendrier de conservation de leur institution, afin de s'assurer que leurs messages soient classés au bon endroit et pour une période de temps appropriée.

Les documents essentiels doivent être sauvegardés. Ils devraient être protégés par des mesures de sécurité propres aux réseaux électroniques et des mesures de sécurité physiques. Il faut aussi en garantir la facilité d'utilisation, même s'ils sont chiffrés, malgré le temps qui passe et les changements technologiques. Il est essentiel de créer, tenir à jour et conserver une documentation du système de courriel et du système de stockage, afin de pouvoir récupérer les données après un sinistre, ou authentifier des courriels lors de demandes dans le cadre d'actions en justice, d'audits ou de l'AIPRP. Les organismes doivent aussi être capables de protéger leurs courriels contre toute divulgation, utilisation, disposition ou destruction inappropriées, et cela, en vertu des obligations découlant de lois et de politiques en vigueur. Il sera peut-être nécessaire, à l'occasion, d'appliquer un ordre de retenue, afin de retarder l'élimination de documents qui pourraient être requis à des fins juridiques.

Résultats attendus

Toutes les institutions du gouvernement fédéral auront obtenu les résultats suivants :

- Les informations contenues dans les courriels et possédant une valeur de conservation permanente pour le gouvernement du Canada ou pour les Canadiens pourront être utilisées, de manière fiable, maintenant et dans les années futures.
- Il sera possible de garantir la facilité d'utilisation des courriels, même s'ils sont chiffrés, malgré le temps qui passe et les changements technologiques.
- Les utilisateurs de courriel devront connaître les calendriers de conservation, lesquels seront appliqués correctement en fonction du contenu des courriels, ou automatiquement en fonction de la classification de ces courriels.

- Les courriels devront être protégés de manière fiable contre toute divulgation, utilisation, disposition ou destruction inappropriées, et cela, en vertu des obligations découlant de lois et de politiques en vigueur.

5.1. Éviter de procéder à des purges indiscriminées dans les systèmes de courriel

Les utilisateurs, tout comme les administrateurs de systèmes ou de réseaux, ne devraient jamais procéder à des purges périodiques et indiscriminées de messages dans les systèmes de courriel, qu'elles soient manuelles ou automatiques. La disposition ou l'élimination des courriels devrait toujours se faire conformément à un calendrier de conservation approuvé par l'institution, et non pas simplement quand la boîte aux lettres est « pleine » ou que les messages dépassent une limite de temps arbitraire.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

5.2. Gérer les courriels de façon à en permettre l'accès aux personnes autorisées

Afin de permettre à l'institution de poursuivre son travail, les systèmes et programmes de gestion des courriels devraient avoir la flexibilité nécessaire pour permettre au personnel autorisé d'avoir accès aux courriels d'un employé, lorsque cette personne est absente.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

5.3. Enlever le chiffrement avant de quitter une institution

Le chiffrement des messages et de leurs pièces jointes doit être enlevé avant que l'utilisateur ne quitte son emploi dans une institution.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

.

5.4. Enlever le chiffrement avant de transférer les courriels à Bibliothèque et Archives Canada

Le chiffrement devrait être enlevé des courriels et de leurs pièces jointes avant leur transfert à Bibliothèque et Archives Canada. L'utilisateur devrait retirer lui-même le chiffrement du message, s'il travaille encore pour l'organisme. Autrement, c'est le gestionnaire des opérations responsable de la section de l'organisme où le message a été chiffré qui devrait enlever le chiffrement; dans ce cas, il est possible que soient requis l'avis d'un spécialiste en gestion de l'information et le soutien d'un administrateur de réseau ou de système. En l'absence de l'utilisateur et du gestionnaire des opérations, le spécialiste en gestion de l'information devrait avoir l'autorisation de décoder le message, avec l'aide d'un administrateur de réseau ou de système.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

.

5.5. Garantir la sécurité des systèmes qui soutiennent les fonctions de courriel

Les programmes et les systèmes de courriel devraient s'appuyer sur des réseaux protégés par des technologies éprouvées, tels les coupe-feux, et une protection devrait être fournie contre les menaces suivantes (liste non exhaustive) :

- Accès non autorisé
- Virus, vers, chevaux de Troie, ActiveX et Applets Java

- Pourriels
- Mouchards, publiciels et fenêtres contextuelles
- Toute autre menace invasive qui pourrait apparaître

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

5.6. Utiliser des mots de passe, les changer régulièrement et les garder secrets

Les administrateurs de réseaux ou de systèmes devraient instaurer des systèmes de mots de passe et veiller à ce que les utilisateurs se conforment aux politiques concernant les mots de passe. Une première démarche consiste à protéger les mots de passe eux-mêmes. À cette fin, les administrateurs doivent changer les mots de passe par défaut installés par le fabricant du système d'exploitation ou du logiciel. Ces mots de passe par défaut sont bien connus des pirates informatiques, ce qui leur permet d'avoir accès aux centaines ou milliers de mots de passe en usage dans l'organisation.

Les utilisateurs devraient choisir des mots de passe difficiles à deviner – il faut éviter le nom de ses enfants, de son chien, de son équipe de sport favorite, de célébrités locales, etc. Les mots de passe devraient se conformer aux normes et caractéristiques établies par l'institution. Les utilisateurs devraient aussi garder secrets leurs mots de passe et les changer périodiquement.

Suggestions visant à améliorer la sécurité des mots de passe **Source : Manuel canadien de la sécurité des technologies de l'information – section 16.1.1 – Mots de passe** **Disponible auprès du Centre de la sécurité des télécommunications Canada**	
Générateurs de mots de passe	Si les utilisateurs n'ont pas la possibilité de générer leur propre mot de passe, il leur est impossible de choisir des mots de passe faciles à mémoriser. Certains générateurs ne créent que des mots de passe ne comprenant aucun mot, mais étant prononçables pour pouvoir être mémorisés par les utilisateurs. Cependant, les utilisateurs ont tendance à écrire les mots de passe difficiles à mémoriser.
Phrases servant de mots de passe	L'utilisation d'une courte phrase au lieu d'un simple mot peut améliorer la résistance des mots de passe. La phrase est habituellement facile à mémoriser et donne de bons résultats en matière de sécurité si les phrases évidentes sont évitées.

Suggestions visant à améliorer la sécurité des mots de passe Source : Manuel canadien de la sécurité des technologies de l'information – section 16.1.1 – Mots de passe Disponible auprès du Centre de la sécurité des télécommunications Canada	
Nombre limité de tentatives d'entrer en communication	De nombreux systèmes d'exploitation peuvent être configurés pour effectuer un verrouillage après un certain nombre de tentatives d'entrer en communication infructueuses. Ce procédé permet de rendre les mots de passe impossibles à deviner.
Attributs de mot de passe	Les utilisateurs peuvent être priés, ou forcés par le système TI, de sélectionner des mots de passe 1) d'une certaine longueur minimale; 2) comprenant des caractères spéciaux; 3) n'ayant aucun rapport avec leur identification; 4) qui ne font pas partie d'un dictionnaire en ligne. Les mots de passe ainsi créés sont plus difficiles à deviner (mais ils ont plus tendance à être écrits).
Changement des mots de passe	Le changement régulier des mots de passe peut amoindrir les dommages causés par l'utilisation de mots de passe volés et rendre plus difficiles les attaques en force visant à pénétrer dans les systèmes TI. Il est cependant possible que des changements trop fréquents finissent par irriter les utilisateurs.
Protection technique du fichier du mot de passe	Le contrôle d'accès et le chiffrement unidirectionnel peuvent être utilisés pour protéger le fichier du mot de passe lui-même. Il est cependant indispensable de ne pas oublier que toutes les protections peuvent être annulées par des attaques suffisamment sophistiquées.

Source : http://www.cse-cst.gc.ca/publications/gov-pubs/itsg/itsg-f.html

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

5.7. Protéger les systèmes contre les pertes ou les dommages

Les systèmes de courriels et les réseaux qui les soutiennent devraient être protégés contre les pertes ou les dommages pouvant provenir de plusieurs sources, dont les suivantes (liste non exhaustive) :

- Menaces physiques aux édifices et aux équipements informatiques
- Désastres naturels et menaces environnementales

- Défaillances des systèmes ou des équipements informatiques
- Vulnérabilité des supports
- Vulnérabilité des communications
- Absence ou perte de documentation
- Erreur humaine
- Autres menaces éventuelles pouvant émerger

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

5.8. Employer le bon niveau de classification de sécurité

Lors de la création, de l'envoi ou du stockage d'un courriel de nature sensible, protégée ou secrète, l'utilisateur devrait s'assurer que la classification de sécurité de ce courriel n'est pas supérieure à celle du système ayant servi à le créer, l'envoyer ou le stocker.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

5.9. Établir des processus obligatoires pour créer, supprimer et suspendre les comptes de courriel au moment opportun

Les programmes et systèmes de courriel devraient comporter des processus pour, au moment opportun, créer un compte de courriel à l'arrivée d'un employé ou d'un contractuel, le supprimer à son départ, le geler ou le suspendre pour toute raison valable.

Ces processus devraient décrire ce que les employés, les gestionnaires, les dirigeants, les administrateurs de réseaux et les spécialistes en sécurité de l'information devraient faire en diverses circonstances (et à quelle vitesse ils devraient intervenir).

« Au moment opportun » ne signifie pas nécessairement « tout de suite ». Dans le cas d'un employé qui passe d'un organisme à un autre, il est sans doute préférable de garder son compte actif tant qu'un autre compte n'a pas été ouvert chez son nouvel employeur. Dans de telles circonstances, il serait avisé de consulter un spécialiste en sécurité de l'information quant à la meilleure façon de procéder.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

5.10. Contrôler les droits d'accès aux comptes et aux dossiers de courriel

L'accès aux informations et aux documents contenus dans les comptes et les dossiers de courriel devrait être limité à ceux qui en ont besoin pour leur travail.

La plupart des personnes ayant un accès autorisé à leur boîte aux lettres individuelle devraient pouvoir créer, modifier et supprimer des messages, ainsi que les classer dans des dossiers.

La capacité de lire, de marquer, « d'envoyer au nom de », ou d'ajouter des messages à des dossiers peut être déléguée à un ou plusieurs collègues de travail au sein de la même unité. Des règles devraient être mises en place pour encadrer de telles délégations.

Certaines personnes autorisées peuvent recevoir une autorisation de « lecture seulement ». Afin de limiter les risques de perdre des informations importantes, seul un nombre restreint de personnes devrait avoir la possibilité de supprimer des messages dans un dossier.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

.

5.11. Utiliser des mesures de protection et d'authentification des messages

Les programmes et systèmes de gestion des courriels devraient offrir des mesures de protection et d'authentification des messages afin d'empêcher les utilisateurs ou les administrateurs de modifier un message une fois qu'il a été envoyé à au moins un destinataire, ceci afin de faciliter l'authentification et le contrôle des versions.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

5.12. Effectuer régulièrement des copies de sécurité aux fins de récupération en cas de sinistre

Les programmes et systèmes de courriel devraient effectuer régulièrement des copies de sécurité, de manière uniforme, afin de répondre aux besoins opérationnels de l'organisme.

- Les copies de sécurité devraient être vérifiées afin de s'assurer qu'elles ont été faites correctement.
- Les copies de sécurité devraient être gardées dans un autre édifice.
- Les copies de sécurité devraient être recyclées régulièrement, conformément au calendrier de conservation de l'institution.
- Les procédures de copie devraient être documentées et gérées de façon à prouver qu'elles répondent aux normes.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

5.13. Utiliser la signature numérique s'il y a lieu

La signature numérique devrait être utilisée dans une correspondance ou une transaction, lorsque le destinataire a besoin de savoir, hors de tout doute, que le message provient d'un expéditeur fiable, que le message n'a pas été modifié et que l'expéditeur ne pourra jamais nier qu'il l'a envoyé.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaire des opérations	Dirigeants

5.14. Enlever les signatures numériques servant à empêcher l'accès aux courriels avant de les transférer à Bibliothèque et Archives Canada

Normalement, une signature numérique n'empêche pas d'avoir accès au contenu, au contexte ou à la structure d'un courriel. Les signatures numériques qui empêcheraient cet accès devraient être enlevées des messages destinés à être transférés à Bibliothèque et Archives Canada.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

5.15. Ne pas employer de signature numérisée pour signer un courriel

Les utilisateurs ne devraient jamais employer de signature numérisée pour signer un courriel, car une telle signature n'authentifie aucunement le courriel. De plus, le risque existe que cette signature soit copiée et intégrée à des documents falsifiés.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

5.16. Utiliser le chiffrement s'il y a lieu

Le chiffrement peut être utilisé, s'il y a lieu, pour accroître la sécurité d'un courriel et de ses pièces jointes durant la période de stockage ou lors d'une transmission.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

5.17. Employer le stockage de proximité pour la conservation à long terme des courriels

Les courriels, ainsi que leurs métadonnées et pièces jointes, qui doivent être conservés pendant un certain temps devraient être stockés dans un système électronique de gestion de l'information, distinct du système de courriel.

Les courriels, leurs métadonnées et pièces jointes devraient être conservés ensemble; si ces éléments sont stockés séparément, il devrait être possible de reconstituer la relation qui les unit, de sorte que l'authenticité et l'intégrité de ces éléments, et leur relation, puissent être démontrées en cour.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

5.18. Éviter de conserver des copies papier de courriels dont l'original électronique existe encore

Au gouvernement du Canada, on ne privilégie pas la conservation de copies papier de documents électroniques. Toutefois, la conservation de courriels sur support papier peut être appropriée dans le cas de petits organismes disposant de ressources technologiques limitées. Cette méthode peut aussi convenir pour les documents à haut risque.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes de la gestion de l'information	Gestionnaires des opérations	Dirigeants

5.19. Protéger les courriels en protégeant les supports de conservation

Un programme de gestion des courriels devrait être capable de protéger les supports de conservation au même titre que les informations électroniques, et devrait régulièrement vérifier les données stockées afin de détecter d'éventuelles pertes d'informations.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

5.20. Protéger les courriels de l'obsolescence

Un programme de gestion des courriels devrait protéger ceux-ci contre l'obsolescence des logiciels et des équipements requis pour lire les messages et leurs pièces jointes.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

5.21. Constituer, tenir à jour et conserver une documentation relative au système de courriel

La documentation relative à un système de gestion des courriels devrait pouvoir, au moment opportun, fournir des preuves raisonnables de la condition du système, ainsi que de l'authenticité et de l'intégrité des courriels, de leurs métadonnées et pièces jointes au cours de la période pertinente dans le contexte de l'action juridique.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

5.22. Conserver en permanence la documentation du système de courriel

La documentation de système devrait être considérée comme un document gouvernemental à conservation permanente, et devrait donc être traitée et entreposée en conséquence.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

5.23. Gérer des délais de conservation différents pour les courriels et leurs pièces jointes

Le système de gestion des courriels doit être configuré de façon à pouvoir gérer à la fois un message dont le délai de conservation vient tout juste de commencer, et une pièce jointe dont le délai est sur le point d'expirer, que les messages et leurs pièces jointes soient conservés ensemble ou séparément. Il convient de rappeler que les délais de conservation sont établis en fonction du

contenu de l'information et non en fonction du système qui a servi à créer, transmettre ou stocker cette information. Cela constitue un problème difficile et pose de réels défis techniques. Il est fortement recommandé de consulter un conseiller juridique.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

5.24. Appliquer un ordre de retenue, au besoin, pour retarder l'élimination d'un document

Les systèmes et programmes de gestion des courriels devraient avoir la capacité de repérer les courriels et l'information associée destinés à être éliminés afin, au besoin, de les isoler et de les protéger contre une destruction, qu'elle soit bien ou mal intentionnée, ou accidentelle.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

6. Les institutions doivent disposer de leurs courriels conformément aux lois et politiques pertinentes

En vertu des articles 12 (1) et 13 (1) de la Loi sur la Bibliothèque et les Archives du Canada (2004), aucun document gouvernemental ne peut être éliminé sans une autorisation écrite du bibliothécaire et archiviste du Canada. Il est important d'éliminer régulièrement les courriels éphémères et les copies de courriels (incluant les copies latentes, c'est-à-dire supprimées, mais non écrasées). Cependant, il est essentiel de pouvoir empêcher l'élimination ou la modification de documents requis (ou pouvant être requis) dans le cadre d'un audit, d'une action en justice ou d'une demande d'information en vertu de l'AIPRP.

Résultats attendus

Toutes les institutions du gouvernement fédéral auront obtenu les résultats suivants :

- Il sera possible de démontrer un degré élevé de conformité aux calendriers de conservation institutionnels, aux autorisations de disposer des documents, approuvées par Bibliothèque et Archives Canada, et aux autres obligations découlant de lois et de politiques, en vue d'assurer au moment opportun l'élimination des courriels qui ne sont plus utiles à l'organisation.
- L'information qui, selon l'institution, possède une valeur historique sera systématiquement transférée à Bibliothèque et Archives Canada.

6.1. Obtenir une autorisation de disposition des courriels

Le bibliothécaire et archiviste du Canada a l'autorité nécessaire pour approuver la disposition de tout courriel sous le contrôle d'une institution gouvernementale et peut déléguer cette autorité à un ou plusieurs responsables dans l'institution.

Le bibliothécaire et archiviste du Canada a le pouvoir d'accorder une autorisation de disposer des documents (ADD) à une institution. Le bibliothécaire et archiviste du Canada peut aussi accorder une autorisation pluri-institutionnelle de disposer des documents (APDD) qui permet l'élimination de documents communs à plusieurs institutions.

Les responsables peuvent à leur tour déléguer aux utilisateurs le pouvoir de prendre des décisions concernant l'élimination des courriels qu'ils créent ou reçoivent, mais cette délégation doit être faite par écrit, avec référence aux présentes Lignes directrices pour la gestion des courriels.

Une infraction aux dispositions de la Loi sur la Bibliothèque et les Archives du Canada est punissable sur déclaration de culpabilité par procédure sommaire (amende / prison).

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

6.2. Éliminer les copies de courriels (incluant les copies latentes) au moment opportun

Les programmes et systèmes de courriel devraient pouvoir repérer les fichiers de courriels à éliminer conformément au calendrier de conservation, où qu'ils se trouvent dans l'organisation, et permettre au personnel autorisé de les détruire de telle manière qu'ils ne puissent jamais être reconstitués.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

6.3. Empêcher la destruction ou la modification de documents qui pourraient être requis dans le cadre d'un audit, d'une action en justice ou de l'AIPRP

Les programmes et systèmes de gestion des courriels devraient pouvoir protéger les courriels et l'information associée, soit le message lui-même, ses métadonnées et pièces jointes, de toute destruction bien ou mal intentionnée, ou accidentelle, et de toute spoliation (terme juridique signifiant dommage ou altération).

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

7. Les institutions doivent réexaminer périodiquement l'efficacité de leurs politiques et pratiques en matière de courriel et apporter des améliorations au besoin

Les systèmes de courriel évoluent très rapidement. L'ajout de nouvelles caractéristiques et de nouveaux services, et une meilleure compatibilité avec d'autres modes de communication engendrent sans cesse de nouvelles formes d'utilisation. Les institutions doivent régulièrement examiner l'efficacité de leurs politiques et pratiques en matière de courriel afin de s'assurer qu'elles atteignent les objectifs visés.

Résultats attendus

Toutes les institutions du gouvernement fédéral auront obtenu les résultats suivants.

- Des cadres de responsabilisation seront en place afin de garantir une gestion efficace des courriels.
- Les risques, faiblesses et autres problèmes importants en matière de gestion seront identifiés, documentés et signalés, et des correctifs seront apportés s'il y a lieu.

7.1. Évaluer l'efficacité de la gestion des courriels

C'est le spécialiste en gestion de l'information (GI) qui a la responsabilité première de procéder à une évaluation périodique détaillée de la gestion des courriels dans son institution et de formuler des recommandations en vue de son amélioration. Cependant, tous les employés de l'organisation ont une part de responsabilité dans la gestion du courriel. Par conséquent, les utilisateurs, les administrateurs de réseaux ou de systèmes, les gestionnaires des opérations et les dirigeants devraient régulièrement évaluer de quelle manière ils pourraient, en tant qu'individus, contribuer plus efficacement à la gestion des courriels. Les institutions devraient mettre à la disposition de leurs employés un endroit accessible où les leçons apprises pourraient être rassemblées et partagées.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

8. Chaque personne oeuvrant au sein du gouvernement fédéral doit comprendre ses responsabilités en matière de gestion des courriels

Résultats attendus

Toutes les institutions du gouvernement fédéral auront obtenu les résultats suivants.

- Tous les employés d'une institution fédérale, incluant les agents et contractuels engagés par cette institution, comprendront leurs rôles et responsabilités en matière de gestion des courriels.
- Ces personnes appliqueront correctement à la gestion des courriels les principes de gestion du cycle de vie de l'information.
- Ces personnes veilleront à ce que les courriels soient conservés sur un support de stockage et dans un endroit appropriés, et durant une période de temps appropriée. Elles respecteront les règles d'étiquette de l'institution en matière de courriel.

8.1. Responsabilités des utilisateurs

Afin de contribuer efficacement à la gestion des courriels, les utilisateurs devraient connaître et comprendre les lois, règlements, normes, lignes directrices, politiques et procédures touchant le courriel, et devraient utiliser et gérer leurs courriels en conséquence.

L'information destinée aux utilisateurs peut prendre la forme de documents, de matériel pédagogique, d'accompagnement individuel ou de cours formels, et peut être offerte sur différents supports, et de différentes manières, selon le choix de l'institution. C'est l'institution qui doit fournir l'information à ses employés. Si ce n'est pas le cas, ceux-ci peuvent en faire la demande.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

8.2. Responsabilités des administrateurs de réseaux ou de systèmes

Les administrateurs de réseaux devraient fournir l'infrastructure technique nécessaire à la gestion des courriels, concevoir et appliquer des procédures de sauvegarde et de récupération en cas de sinistre, fournir des mécanismes de sécurité en TI et sur Internet à la fine pointe, contrôler et surveiller l'accès à l'information et aux documents.

Les administrateurs de réseaux devraient surveiller l'utilisation du courriel afin d'évaluer le respect des politiques et des Lignes directrices pour la gestion des courriels et, s'il y a lieu, enquêter lorsqu'il y a des soupçons d'utilisation abusive du courriel.

Les administrateurs de réseaux devraient créer, tenir à jour et conserver une documentation détaillée sur le système de courriel et les informations qu'il contient. Cette documentation devrait suffire à prouver l'authenticité et l'intégrité de tout courriel ou information associée, produit en preuve lors d'une action en justice.

Les administrateurs de réseaux devraient veiller à ce que les courriels relatifs aux activités organisationnelles ne soient pas stockés dans un dépôt non autorisé.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

8.3. Responsabilités des spécialistes en gestion de l'information

Les spécialistes en gestion de l'information assument généralement de très larges responsabilités et ne sont pas affectés exclusivement à la gestion des courriels. Cependant, ces responsabilités touchant la gestion de l'information en général, s'étendent bien entendu à la gestion des courriels.

> Un spécialiste en gestion de l'information dirige et soutient une gestion de l'information efficace et efficiente au sein d'une organisation, à partir de la planification et du développement de systèmes jusqu'à l'élimination ou à la conservation permanente des documents. (Paraphrase d'une définition sur le portail GI du gouvernement du Canada) :
>
> (Source: http://www.informationmanagement.gc.ca/index_f.asp)

La Politique sur la gestion de l'information du Conseil du Trésor précise que les spécialistes en gestion de l'information – dont les bibliothécaires, les archivistes, les responsables de l'accès à l'information et de la protection des renseignements personnels, et les spécialistes en gestion des documents – contribuent à la gestion de

l'information :

(a) en fournissant conseils, outils, procédures, normes et lignes directrices conformes aux orientations formulées par le Secrétariat du Conseil du Trésor du Canada et Bibliothèque et Archives Canada;

(b) en identifiant les besoins en matière d'information du personnel oeuvrant en technologie de l'information, afin de soutenir le développement et l'utilisation de procédures, systèmes, normes et outils en technologie de l'information;

(c) en évaluant les besoins en matière de ressources et de formation en gestion de l'information.

(Source : http://www.solutions.gc.ca/oro-bgc/rep/im-gi/intro_f.asp)

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

8.4. Responsabilités des gestionnaires des opérations

Les gestionnaires devraient identifier les besoins des employés en matière de formation à la gestion des courriels et leur allouer du temps, pendant les heures de travail, pour leur permettre de suivre une formation appropriée.

Les gestionnaires devraient veiller à ce que le personnel se conforme aux présentes Lignes directrices pour la gestion des courriels, notamment les procédures de réception et de départ de même que les procédures d'orientation, la classification et le stockage adéquats des documents et de l'information, et l'application de délais de conservation appropriés.

Les gestionnaires devraient s'assurer que les employés aient à leur disposition tous les documents de référence concernant la gestion des courriels, ou qu'ils sachent où et comment les obtenir au besoin.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

8.5. Responsabilités des dirigeants

Les dirigeants devraient définir les orientations stratégiques en matière de courriel, et guider l'élaboration et l'adoption d'une politique institutionnelle sur la gestion des courriels.

Un dirigeant qui assume également le rôle de gardien des documents devrait veiller à ce que les courriels faisant l'objet de demandes en vertu de lois d'accès ou dans le cadre d'actions en justice ne soient pas détruits.

Les dirigeants devraient accorder un financement adéquat aux programmes et systèmes de gestion des courriels, afin de garantir leur conformité aux politiques et lois en vigueur, et aux présentes Lignes directrices et recommandations pour la gestion des courriels.

Les dirigeants devraient s'assurer que de bonnes formations en gestion des courriels soient préparées et offertes aux employés, que la participation des employés soit consignée et l'information conservée, et que le matériel pédagogique et de référence soit disponible sur différents supports.

Les dirigeants doivent s'assurer que les employés reçoivent les présentes Lignes directrices pour la gestion des courriels et les recommandations associées, et que ceux-ci confirment par écrit les avoir bien reçues et comprises; cette confirmation écrite sera conservée par la suite.

Les dirigeants devraient réexaminer régulièrement les politiques et procédures en matière de gestion des courriels, afin d'en évaluer l'efficacité, résoudre les éventuels problèmes et apporter des améliorations.

Partie ou parties responsables de la mise en œuvre ou de l'application de la recommandation				
Utilisateurs	Administrateurs de réseaux ou de systèmes	Spécialistes en gestion de l'information	Gestionnaires des opérations	Dirigeants

Annexe A. RÔLES ET RESPONSABILITÉS

Le tableau ci-dessous illustre le partage des responsabilités entre les divers intervenants, dans la mise en oeuvre des présentes Lignes directrices pour la gestion des courriels et des recommandations associées.

- Les utilisateurs (UTIL)
- Les administrateurs de systèmes ou de réseaux (ASYS)
- Les spécialistes en gestion de l'information (SGI)
- Les gestionnaires des opérations (GOP)
- Les dirigeants (DIR)

La responsabilité est indiquée par un crochet à l'intersection d'un intervenant et d'une ligne directrice ou d'une recommandation.

Lignes directrices	UTIL	ASYS	SGI	GOP	DIR
0. Introduction au Lignes directrices pour la gestion des courriels					
0.2.Lignes directrices	✓	✓	✓	✓	✓
0.3. Pourquoi ces lignes directrices s'appliquent-elles à tout le monde?	✓	✓	✓	✓	✓
0.4. Quels sont les résultats attendus?	✓	✓	✓	✓	✓
0.5. Pourquoi la gestion des courriels est-elle si importante?	✓	✓	✓	✓	✓
0.6. Domaines où les lignes directrices ne s'appliquent pas	✓	✓	✓	✓	✓
0.7. Feuille de route pour se conformer aux lignes directrices	✓	✓	✓	✓	✓
0.8. Cycle de vie de l'information électronique	✓	✓	✓	✓	✓
0.9. Définitions	✓	✓	✓	✓	✓
1. Les institutions doivent se doter d'un plan pour gérer les courriels 1.0. Recommandations					
1.1. Gérer les programmes et les systèmes de courriel de manière intégrée	✓	✓	✓		
1.2. Offrir des programmes de sensibilisation et de formation à la gestion des courriels					✓

Lignes directrices	UTIL	ASYS	SGI	GOP	DIR
1.3. Utiliser divers supports pour sensibiliser et former à la gestion des courriels					✓
1.4. Vérifier que les Lignes directrices pour la gestion des courriels, ainsi que les politiques et procédures associées ont bien été distribuées, lues et comprises					✓
1.5. Conserver des dossiers sur les activités de formation et sur la participation					✓
2. Les institutions doivent recueillir et conserver tous les courriels relatifs à leurs activités organisationnelles					
2.0. Recommandations					
2.1. Créer, expédier et stocker les courriels de manière structurée	✓	✓	✓		
2.2. Recevoir et stocker les courriels de manière structurée	✓	✓	✓		
2.3. Gérer les boîtes aux lettres et les dossiers individuels sur une base régulière	✓				
2.4. Garder un seul exemplaire de chaque courriel	✓	✓	✓	✓	✓
2.5. Gérer et conserver les pièces jointes aux courriels		✓	✓		
2.6. Considérer les courriels comme des biens, soumis au contrôle juridique du gouvernement du Canada	✓	✓	✓	✓	✓
2.7. Utiliser avec modération les listes de diffusion institutionnelles	✓				
2.8. Fournir un bloc-signature et les coordonnées de la personne-ressource		✓	✓		
2.9. Ajouter un avis de confidentialité ou de non-responsabilité, s'il y a lieu	✓	✓		✓	✓
2.10. Ajouter un avis d'opinion personnelle, s'il y a lieu	✓	✓			✓
2.11. Éviter d'utiliser la fonction "Répondre à tous"	✓				
3. Les institutions doivent classer les courriels relatifs à leurs activités selon un plan de classification basé sur leurs exigences organisationnelles					
3.0. Recommandations					

Lignes directrices	UTIL	ASYS	SGI	GOP	DIR
3.1. Maintenir et utiliser un système structuré et efficace de classement des courriels	✓	✓	✓		
3.2. Déterminer où classer la « copie officielle »		✓	✓		✓
3.3. Conserver les métadonnées associées aux courriels		✓	✓		
3.4. Classifier et classer les courriels systématiquement et fréquemment	✓				
3.5. Gérer le stockage en ligne temporaire des courriels	✓	✓			
3.6. Utiliser à une seule fin les boîtes aux lettres communes ou publiques et les dossiers de courriels	✓	✓	✓	✓	
3.7. Limiter le contenu des courriels à un seul sujet	✓				
3.8. Décrire l'objet d'un courriel en termes clairs et significatifs	✓				
3.9. Prévoir un système d'indexation des courriels		✓	✓		
3.10. Prévoir un mécanisme permettant de suivre le fil conducteur reliant les courriels entre eux (*threading*)		✓	✓		
4. Les institutions doivent veiller à ce que l'utilisation du courriel contribue à la réalisation d'activités correspondant à leurs objectifs organisationnels 4.0. Recommandations					
4.1. Ne pas utiliser le courriel pour traiter de sujets sensibles, personnels, protégés ou secrets, sauf dans les cas autorisés et en respectant les normes de sécurité en vigueur	✓				
4.2. Utiliser les journaux d'exploitation pour constituer une piste de vérification et veiller au respect des règles		✓	✓		
4.3. Afficher les noms dans les en-têtes et les adresses de courriel		✓			
4.4. Être prêt à divulguer un courriel en preuve, sous forme électronique		✓	✓		
4.5. Surveiller la performance des activités de découverte et de disposition des courriels		✓	✓	✓	

Lignes directrices	UTIL	ASYS	SGI	GOP	DIR
5. Les institutions doivent veiller à ce que leurs courriels soient maintenus, protégés et conservés selon des calendriers de conservation appropriés 5.0. Recommandations					
5.1 Éviter de procéder à des purges indiscriminées dans les systèmes de courriels		✓			
5.2. Gérer les courriels de façon à en permettre l'accès aux personnes autorisées	✓	✓		✓	
5.3. Enlever le chiffrement avant de quitter une institution	✓				
5.4. Enlever le chiffrement avant de transférer les courriels à Bibliothèque et Archives Canada		✓	✓		
5.5. Garantir la sécurité des systèmes qui soutiennent les fonctions de courriel		✓			
5.6. Utiliser des mots de passe, les changer régulièrement et les garder secrets	✓	✓			
5.7. Protéger les systèmes contre les pertes et les dommages		✓	✓		
5.8. Employer le bon niveau de classification de sécurité				✓	✓
5.9. Établir des processus obligatoires pour créer, supprimer et suspendre les comptes de courriel au moment opportun	✓	✓		✓	
5.10. Contrôler les droits d'accès aux comptes et aux dossiers de courriel	✓	✓			
5.11. Utiliser des mesures de protection et d'authentification des messages		✓			
5.12. Effectuer régulièrement des copies de sécurité aux fins de récupération en cas de sinistre		✓			
5.13. Utiliser la signature numérique s'il y a lieu	✓	✓	✓	✓	✓
5.14. Enlever les signatures numériques servant à empêcher l'accès aux courriels avant de les transférer à Bibliothèque et Archives Canada		✓	✓		
5.15. Ne pas employer de signature numérisée pour signer un courriel	✓				
5.16. Utiliser le chiffrement s'il y a lieu	✓	✓	✓	✓	✓

Lignes directrices	UTIL	ASYS	SGI	GOP	DIR
5.17. Employer le stockage de proximité pour la conservation à long terme des courriels		✓	✓		
5.18. Éviter de conserver des copies papier de courriels dont l'original électronique existe encore	✓	✓	✓		
5.19. Protéger les courriels en protégeant les supports de conservation		✓	✓		
5.20. Protéger les courriels de l'obsolescence		✓	✓		
5.21. Constituer, tenir à jour et conserver une documentation relative au système de courriel		✓			
5.22. Conserver en permanence la documentation du système de courriel		✓	✓		
5.23. Gérer des délais de conservation différents pour les courriels et leurs pièces jointes		✓	✓		
5.24. Appliquer un ordre de retenue, au besoin, pour retarder l'élimination d'un document	✓	✓	✓		
6. Les institutions doivent disposer de leurs courriels conformément aux lois et politiques pertinentes 6.0. Recommandations					
6.1. Obtenir une autorisation de disposition des courriels	✓	✓	✓		
6.2. Éliminer les copies de courriels (incluant les copies latentes) au moment opportun		✓	✓		
6.3. Empêcher la destruction ou la modification de documents qui pourraient être requis dans le cadre d'un audit, d'une action en justice ou de l'AIPRP		✓	✓		
7. Les institutions doivent réexaminer périodiquement l'efficacité de leurs politiques et pratiques en matière de courriel et apporter des améliorations au besoin 7.0. Recommandations					
7.1. Évaluer l'efficacité de la gestion des courriels			✓		

Lignes directrices	UTIL	ASYS	SGI	GOP	DIR
8. Chaque personne oeuvrant au sein du gouvernement fédéral doit comprendre ses responsabilités en matière de gestion des courriels 8.0. Recommandations					
8.1. Responsabilités des utilisateurs	✓				
8.2. Responsabilités des administrateurs de réseaux ou de systèmes		✓			
8.3. Responsabilités des spécialistes en gestion de l'information			✓		
8.4. Responsabilités des gestionnaires des opérations				✓	
8.5. Responsabilités des dirigeants					✓